나무위키

PGP

최근 수정 시각: 2026-05-28 16:59:05

분류:컴퓨터 보안 | 암호학

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.9 (MingW32)
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

hQEMA//k/q4to5jWAQf/YB21DYVVnEsVWNWSvCcA+/Nae70pRwUVG41R7ilenzYl
kmM9VB4wH/T8l4AgIRqB/XppL7YlL2EnqhdYMChjKaRtYzK5A10cTFgis4S87a/G
kVhBHsAx5hQ7JgWebT1Hfe/OguNrzlT54CaSqlWxM3jbK7w6RfwkRrIUHbl1c0Jy
Vs3CpQpv2dZbNFNmkYo0r+wwWOVoyyDMUeRkNRq32CQltA6YUbz2BIZAEs9KwJTK
M5A5AR6hHjtnKWTYXF0NRgMEey12UeVhKyqqLA0l0SX8gICZ1kBHnbRe5Eb5LchJ
kY+7vv/3zyAqi22vOR2CnjKglV1L8ia1iHRkTZpWqYUBDAPqdMflbOfpxQEH/0WW
t/BT/abyJLL9jP6SmXBaK5ZsQpcGx41PiWepeKbDWhUn17Sea1T4gATS3Wmtvv0k
mrYAlgoK9UQsKOQpDVk0UGB/AtMrRLQ0T5PmL2pezfZ6IAiHFyvARcMFiuyCEL/1
Y0QVXVaU3SZLtYiHxDDkq7pv/etUTE4Vynn3/mUG7OJ+DDMUSWm6c1HQlQIxPhfV
jWqEX2rO1aqswQ92xkPons4H7gWNDWXYf0bNYktCWOGGvsZW3oouawiSuNuQaHWJ
TQYiFpuIO5kMal2WJupmeMAGGkuNCuXtt7C1ze4hfDl/YSeP55/JQj8AEqCfLG3n
aq8SzlDd4tR3qz4tcLvSwLMBhx1w8wgjrfo3d1Qxtw25hwWe+tVvoPxzTgF3z7ip
6POI/MounrQtK4SGqJ2xDC1l/lCaXdsF2cXyCXCuHSoQ7jzheCn2NvqAHdsx1ttP
+wLm+d9B1VAjsF/p/NFs6R/hHtoDZX4429S8IxnYSlVBm4jzHpOca0wPMMqXGOE9
/vQi8gtXtlG390ejHKjHkHeYX8+j7G7MY0LkYg0Oxdxjza3xXFUQqkPBLfMOFwIo
IDp8dteNaQIM6EPruSazs0oYmUlNxNeBnEMNsfEz/+qfZmCUMnLzJ0d7XPBsHQyk
TLi0Duly/aU0AkV5v5diWbKn7uLChkzppr7OR08a+7u9gsp2HgnHeuoHfQ8EJ1Hf
tfaSIM/N+eUHhAJpyqDY+2TanOXnczjBNbluJmZrEwWNrvXWrqHFwrYn8EYI6AMO
lUKRmcUrN339wbXsqGpRcRQ/9kgySaGNWjmUGRdyhaEFbI0eHV5uZwhGjM1aEGM5
qsORxQ==
=swsB
-----END PGP MESSAGE-----
```

GnuPG로 암호화된 텍스트. 풀려면 암호화에 사용된 공개키와 대칭되는 비밀키가 필요하다.[1]

Pretty Good Privacy.

목차

1. 개요
2. PGP 간단 이해
3. PGP의 의의
   3.1. PGP의 개념 및 역사
   3.2. PGP의 원리
   3.3. 기타
4. PGP (GnuPG) 사용하기
   4.1. 윈도우
      4.1.1. GPG4Win
         4.1.1.1. 주의사항
         4.1.1.2. 프로그램 설치
         4.1.1.3. 키 생성하기
         4.1.1.4. 내 공개키 내보내기
         4.1.1.5. 상대방 공개키 들여오기
         4.1.1.6. 암호문 보내기
         4.1.1.7. 메시지 서명하기
         4.1.1.8. 글자 수 제한이 있는 곳에서 PGP 쓰기
      4.1.2. 컴포넌트
   4.2. 리눅스
   4.3. 맥
   4.4. 안드로이드
   4.5. iOS
5. 사이버셰프 CyberChef
6. PGP 공개키 서버
7. 관련 문서

1. 개요

PGP는 주로 전자메일의 내용을 암호화하는 데 사용되는 공개 키 암호화 방식이다.

2. PGP 간단 이해

철수와 영희가 있다고 가정하자.

공개키: 남에게 공개하는 키.
개인키: 남에게 절대 알려서는 안 되는 키.

철수 공개키: aaaa
철수 개인키: bbbb
영희 공개키: cccc
영희 개인키: dddd

aaaa로 암호화하면 bbbb로 풀 수 있다.
bbbb로 암호화하면 aaaa로 풀 수 있다.
cccc로 암호화하면 dddd로 풀 수 있다.
dddd로 암호화하면 cccc로 풀 수 있다.

이메일 주고받는 과정은 다음과 같다.

철수 -> 영희
1. 철수는 상대방 공개키(cccc)로 이메일 내용을 암호화한다.
2. 철수는 자신의 개인키(bbbb)로 이메일을 서명한다.
3. 철수는 상대방 공개키(cccc)로 이메일을 전송한다.
4. 영희는 자신의 개인키(dddd)로 암호화를 해제하고 내용을 확인한다.(ex. "안녕 영희야")
5. 영희는 상대방의 공개키(aaaa)로 이메일의 서명을 검증한다. 이로써 정말 철수가 보낸 메일임을 확인한다.

영희 -> 철수
1. 영희는 상대방 공개키(aaaa)로 이메일 내용을 암호화한다.
2. 영희는 자신의 개인키(dddd)로 이메일을 서명한다.
3. 영희는 상대방 공개키(aaaa)로 이메일을 전송한다.
4. 철수는 자신의 개인키(bbbb)로 암호화를 해제하고 내용을 확인한다.(ex. "안녕 철수야")
5. 철수는 상대방의 공개키(cccc)로 이메일의 서명을 검증한다. 이로써 정말 영희가 보낸 메일임을 확인한다.

여기서 왜 이메일 내용은 상대방 공개키로 암호화하고, 서명은 내 개인키로 하는지 궁금할 수 있다.

- 내 공개키로 이메일 내용 암호화: 내 개인키를 알아야 암호화를 해제할 수 있는데 상대방이 내 개인키를 모르므로 암호화를 풀 수 없어서 메일보내는 의미가 없어진다.
- 내 개인키로 이메일 내용 암호화: 내 개인키로 암호화할 경우 내 공개키를 이용해 암호화를 해제할 수 있다. 내 공개키는 공개되어 있으므로 개나소나 암호화를 해제할 수 있다. 그래서 암호화하는 의미가 없어진다.
- 상대방 개인키로 이메일 내용 암호화: 애초에 상대방 개인키를 모르므로 불가능하다.
- 내 공개키로 서명: 내 개인키를 알아야 서명을 검증할 수 있는데 상대방이 내 개인키를 모르므로 서명을 검증할 수 없어 서명하는 의미가 없어진다.
- 상대방 공개키로 서명: 내 개인키로 서명하는 것은 오직 나 자신만이 가능하지만, 상대방 공개키로 서명하는 것은 개나소나 가능하다. 그래서 이 메일보낸 사람이 나라는 것을 전혀 증명하지 못하므로 서명하는 의미가 없어진다.
- 상대방 개인키로 서명: 애초에 상대방 개인키를 모르므로 불가능하다.

그러므로 이메일 내용은 상대방 공개키로 암호화하고, 서명은 내 개인키로 한다.

PGP를 이해하는 데 도움이 되었길 바란다.

3. PGP의 의의

3.1. PGP의 개념 및 역사

암호학의 일대 혁명을 가져온 프로그램으로, 1991년 필 짐머만(Phil Zimmermann)[2]이라는 프로그래머가 개발한 전자우편 암호화 프로그램[3]과 그 파생작들을 말한다. 이 프로그램 전까지만 해도 암호화 기능은 정부나 군대, 그리고 정보기관의 전유물이었으나 PGP로 인해서 일반 사람들까지 암호가 퍼지게 되었다. 덕택에 ~~개인 사용자가 암호를 쓴다는 것에~~ 열받은 미국 정부(+NSA)는 PGP의 강력한 암호화 기능이 테러리스트를 도울 수 있다는 이유로 필 지머먼을 군수물자 통제법 위반으로 조사하였으나, 나중엔 조사를 포기하게 된다.

여담으로 1997년 PGP 국제버전인 PGPi 5.0이 개발되었고, 필 지머먼은 이를 국외로 수출하려고 했으나 당시 미국 정부는 암호화 프로그램을 무기로 간주하여 이를 저지한다. 이에 지머먼은 법률을 검토하던 중, 소프트웨어는 수출 금지 항목에 포함되어 있어도, 종이에 인쇄된 책은 수출에 제약이 없다는 점을 발견했다. 법의 허점이라기보다는, 미국에서는 강력한 수정헌법 1조 덕에 출판의 자유가 보장되어 내용이 무엇이든 책으로 배포가 가능했던 것.[4] 그리하여 총 6천여 페이지의 소스코드를 출력하여 12권의 책으로 묶었고, 이를 수출하고 국외에서 지원자를 모집하여 스캐너로 책 페이지의 이미지를 떠서 OCR을 통해 다시 프로그램 소스 코드로 변환하여 컴파일하는 대단한 삽질을 통해 결국 해외 수출에 성공한다. 당시 70여 명의 지원자가 있었다고 한다. 스캔과 OCR 변환, 빌드와 미국 국외에서 출시하기까지 걸린 총 시간은 1000시간 쯤 된다고 한다. 이를 "PGPi Scanning Project"라고 부른다. 이후 개정판 버전이 다시 이러한 과정을 거쳐 수출에 성공했으며, 미 정부가 1999년에 적성국가를 제외한 나머지 국가에 암호화 프로그램이나 장비의 수출을 허가하였으며, 특히 오픈소스 구현체의 경우 사실상 통제가 불가능하다는 판단에 의해 사실상 유예하고 있어 일반적인 상황에서는 문제가 없다.[5]

또한, 암호화 알고리즘을 사용하는 다른 소프트웨어들도 같은 이유로 수출이 제한되어 해외에서는 미국산 소프트웨어에서 대칭키 암호화 알고리즘은 키 길이가 40비트로 제한된 알고리즘을 쓸 수밖에 없었다. 따라서, 한국에서는 전자상거래용으로 SEED라는 128비트 키를 사용하는 독자적인 암호화 알고리즘을 개발해 익스플로러에 ActiveX 형태로 적용했으며, 이때부터 ActiveX와 함께하는 환장할 인증 시스템이 완전히 뿌리내리게 된다. 지금은 ActiveX가 아닌 프로그램 설치 방식으로 대부분 바뀌었지만 시스템에 접근이 불가능한 자바스크립트가 아닌 시스템에 접근이 가능한 추가 기능을 이용한다는 점에서 보안상 취약한 점은 변하지 않는다. 좀 더 최근에는 웹 표준 및 자바스크립트 기반 인증서 시스템과 사설 인증서가 등장하여 조금씩 대체되는 중이다.

3.2. PGP의 원리

자세한 내용은 RSA 암호화 문서나 공개 키 암호화 방식 또는 RSA에 대한 전문서적을 참고.

간단히만 설명하자면, 이메일 내용 자체를 암호화하여 오로지 보내는 사람과 받는 사람만이 그 원문(Plain Text)을 알 수 있도록 하는 암호화 방식을 말한다. 물론 이메일 서비스 제공자(Google, Yahoo, Outlook 등)는 이메일의 전송 과정에서 TLS를 적용하는 등의 기본적인 보안을 제공한다. 하지만 이메일 서비스 제공자 자체를 신뢰할 수 없거나[6], 법원이 발부한 압수수색 영장에 의해 수사상 필요로 인해 이메일 서비스 제공자가 이메일을 수사기관과 법원에 제출해야 하는 경우에는 수사와 관련없는 이메일까지 내용이 그대로 노출될 수밖에 없다.[7] PGP등으로 암호화해서 메일을 송수신했더라도 개인키는 컴퓨터등에 있을 것이고, 송수신 과정에 여러 디지털 흔적이 남으므로 디지털 포렌식을 회피하기란 사실상 힘들다. 일반적인 경우에 이메일 제공자조차 이메일의 원문을 알 수 없도록 암호화를 할 필요가 있었고, 그것이 PGP이다.

PGP의 기능은 크게 인증과 기밀성 보장으로 나눌 수 있다. 인증은 전송하려는 메시지의 해시값에 송신자의 개인키를 이용해 암호화(전자서명)을 수행하는 것으로 달성할 수 있고. 기밀성 보장은 세션키(대칭키)와 송수신자의 비대칭 키를 통한 암호화로 달성할 수 있다.

송신자는 먼저 전송하려는 메시지를 생성한다. 이 메시지를 해시함수를 이용해 해시값을 생성하고 그 해시값을 송신자의 개인키로 암호화하면 이 암호문은 해당 메시지에 대한 전자서명이 된다. 그리고 송신자는 의사난수 생성기 등을 이용해 세션키를 생성하고 메시지와 전자서명을 결합한 값을 세션키로 암호화한다. 세션키는 수신자의 공개키로 암호화하여 세션키로 암호화된 값과 함께 전송한다.

수신자는 전송받은 데이터에서 세션키 부분을 분리해 수신자의 개인키로 복호화하여 세션키를 획득한다. 이 세션키로 나머지 부분을 복호화하고 전자서명과 메시지를 분리하여 여기서 수신자는 메시지 원문을 획득할 수 있다. 여기서 메시지 변조 여부 혹은 송신자 검증을 위해 인증을 수행한다. 전자서명은 송신자의 공개키로 복호화하고 획득한 메시지 평문으로 사전에 공유된 해시 함수를 통해 해시값을 구한다. 직접 얻어낸 해시값과 복호화로 얻어낸 해시값이 동일하다면 이 메시지는 변조되거나 타인이 송신하지 않은 것이다. 그러나 동일하지 않다면 이 메시지는 변조되었거나 타인이 송신한 값이기에 해당 값은 폐기하고 송신자에게 재송신을 요구한다.

3.3. 기타

처음 개발되었을 때 개인 사용자한테는 무료였지만, 현재는 유료로 시만텍에서 판매하고 있다. 그러나 PGP의 한 갈래인 OpenPGP는 현재 인터넷 표준으로 자리매김 하였으며, 이를 이용한 GnuPG같은 여러 프로그램이 등장했다. 당연하게 윈도우나 맥, 리눅스 버전도 존재한다.

리눅스는 패키지 보관소(Repository)에 보관된 소프트웨어를 보관소의 GPG 키를 이용하여 패키지에 문제가 있는지 없는지 확인하며, 몇몇 포럼의 Geek들은 자신이 직접 글을 썼다는 걸 증명하기 위해 PGP를 사용해 사인하거나 암호화하여 글을 작성하기도 하며, 이러한 글은 작성자의 공개키를 바탕으로 PGP를 통해 해독하여 본인인지 아닌지 확인할 수 있다.

4. PGP (GnuPG) 사용하기

- Symantec PGP(상용): http://www.symantec.com/encryption/ [8]
- GnuPG(오픈소스): https://www.gnupg.org

4.1. 윈도우

4.1.1. GPG4Win

GPG4Win 간단한 활용법 2가지@
https://www.gpg4win.org/에서 윈도우용 GPG 프로그램인 GPG4Win을 다운로드 받을 수 있다.

4.1.1.1. 주의사항

아래의 주의사항들이 있다.

1. 아래의 가이드 글은 '철수'가 '영희'에게 암호문 또는 서명된 메시지를 보내는 상황이라고 가정한다.

2. 아래의 가이드 글은 PGP 공개키 서버를 이용하지 않았다.

3. 개인키는 절대로 유출되어서는 안된다. 만약 유출되었다면 즉시 키를 폐기해야 한다. 'BEGIN PGP PRIVATE KEY BLOCK' 문구의 아래 부분이 개인키이다.참고 링크

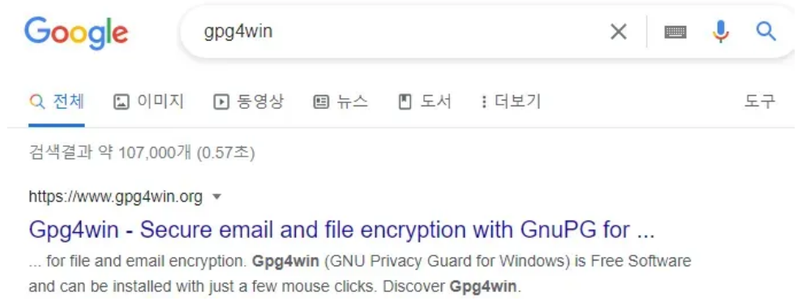
4. PGP는 메시지 내용을 암호화해 줄 수는 있지만 누가(철수) 누구(영희)에게 메시지를 보냈다는 사실을 숨길 수는 없다. 다시말해 PGP는 메타데이터를 숨겨주지는 못한다.

5. PGP 프로그램 중 gpg4usb가 있는데 이 프로그램은 ECDSA/EdDSA(ed25519)를 지원하지 않는다. 그러므로 만약 상대방이 gpg4usb를 쓴다면 무조건 RSA 4096비트를 선택해야 한다.

6. 커뮤니티에 공개키를 입력할 수 있는 공간이 필요하다. 보통 PGP로 소통하는 커뮤니티는 공개키를 입력할 수 있는 프로필란(갤로그 같은 것)이 있다. 상대방에게 PGP로 암호문을 보내고 싶으면 상대방의 프로필란(갤로그 같은 것)을 보고 상대방의 공개키를 알아내면 된다. 디시인사이드의 경우 갤로그의 방명록이 공개키를 게시하기에 적당하지만 안타깝게도 글자수 1000자 제한때문에 갤로그 방명록에 공개키를 게시하기 어렵다.

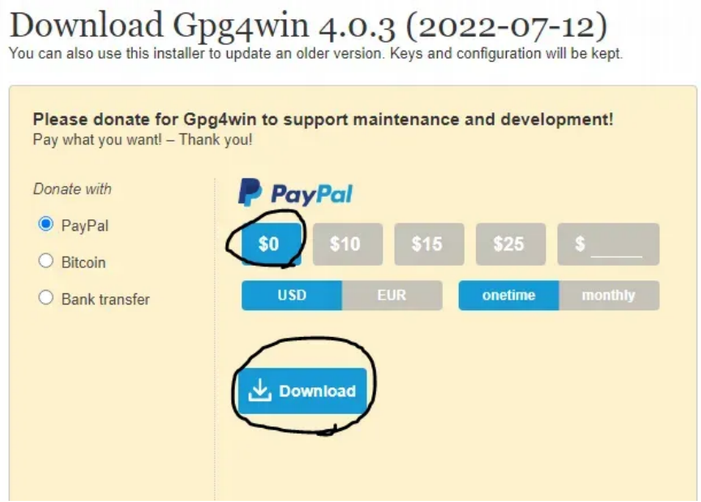
4.1.1.2. 프로그램 설치

1. 철수: GPG4Win 사이트에 들어간다.

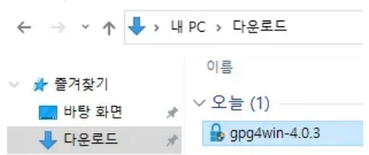


2. 철수: Download 클릭

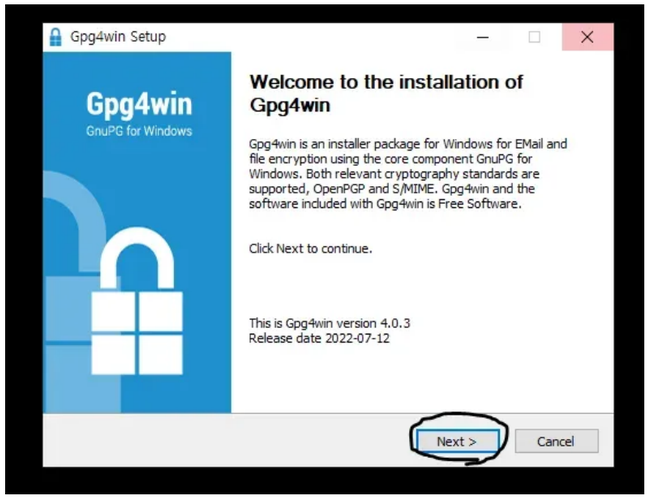
3. 철수: $0 선택하고[9] Download 클릭



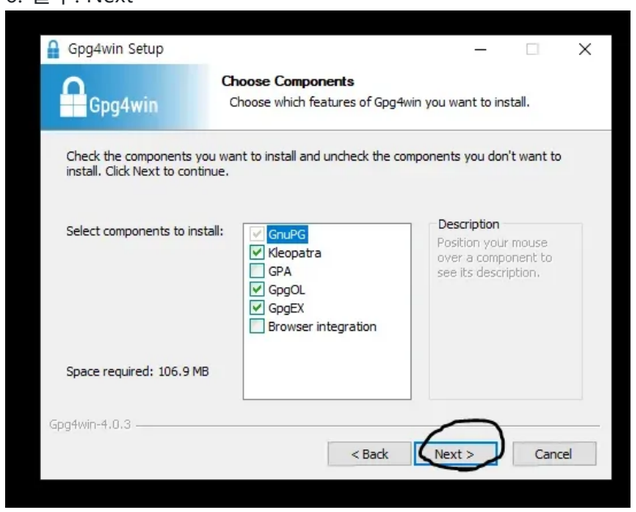
4. 철수: 실행



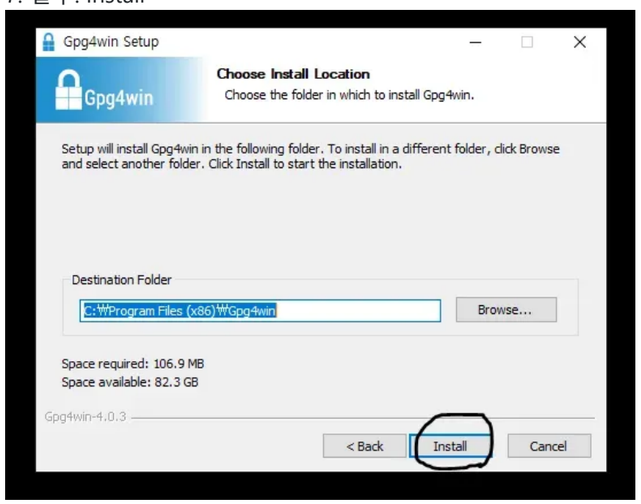
5. 철수: Next


Gpg4win Setup
Gpg4win
GnuPG for Windows
Welcome to the installation of Gpg4win
Gpg4win is an installer package for Windows for EMail and file encryption using the core component GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win is Free Software.
Click Next to continue.
This is Gpg4win version 4.0.3
Release date 2022-07-12
Next >
Cancel

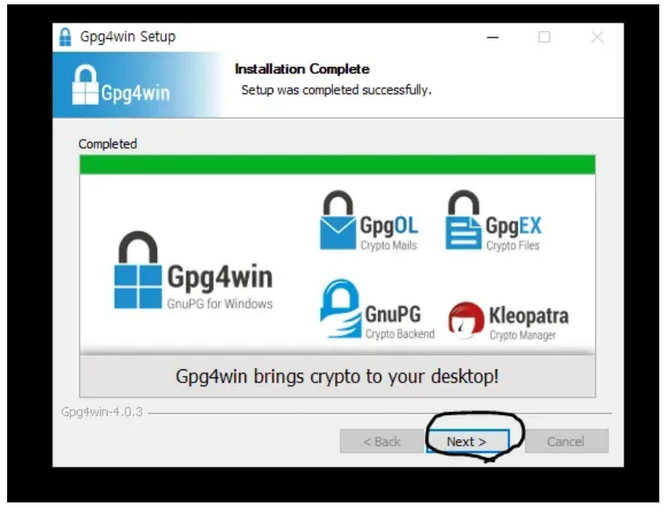
6. 철수: Next



7. 철수: Install


Gpg4win Setup
Gpg4win
Choose Install Location
Choose the folder in which to install Gpg4win.
Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:₩Program Files (x86)₩Gpg4win
Browse...
Space required: 106.9 MB
Space available: 82.3 GB
Gpg4win-4.0.3
< Back
Install
Cancel

8. 철수: Next



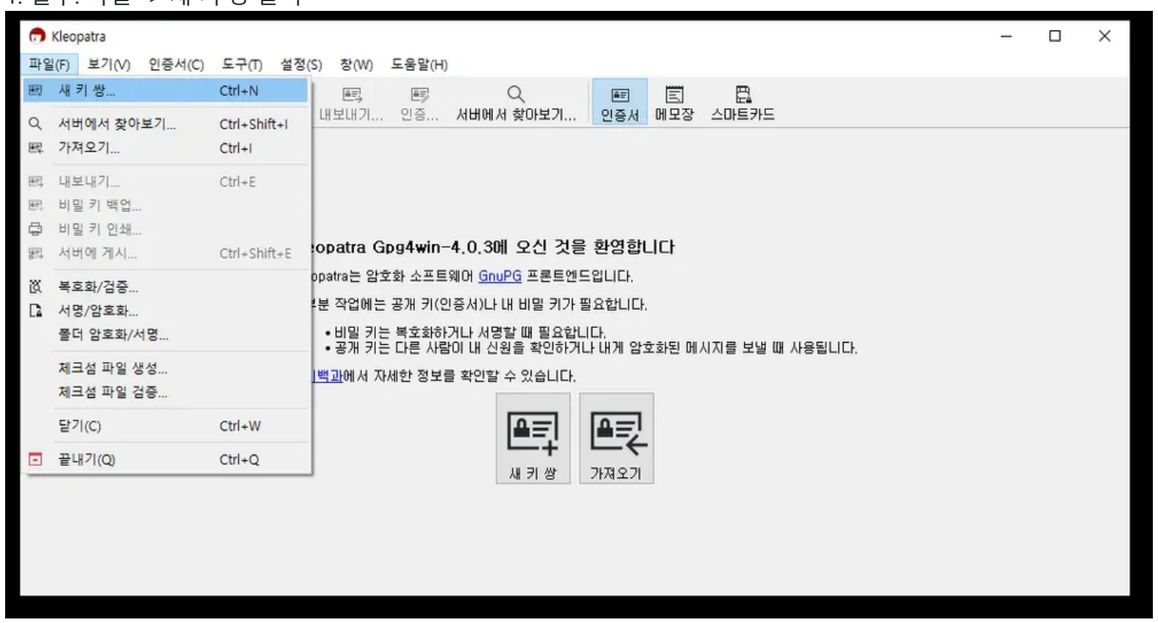
9. 철수: Finish

10. 철수: 전체적인 모습이다.

Kleopatra
파일(F) 보기(V) 인증서(C) 도구(T) 설정(S) 창(W) 도움말(H)
서명/암호화... 복호화/검증... 가져오기... 내보내기... 인증... 서버에서 찾아보기... 인증서 메모장 스마트카드
Kleopatra Gpg4win-4.0.3에 오신 것을 환영합니다
Kleopatra는 암호화 소프트웨어 GnuPG 프론트엔드입니다.
대부분 작업에는 공개 키(인증서)나 내 비밀 키가 필요합니다.
• 비밀 키는 복호화하거나 서명할 때 필요합니다.
• 공개 키는 다른 사람이 내 신원을 확인하거나 내게 암호화된 메시지를 보낼 때 사용됩니다.
위키백과에서 자세한 정보를 확인할 수 있습니다.
새 키 쌍
가져오기

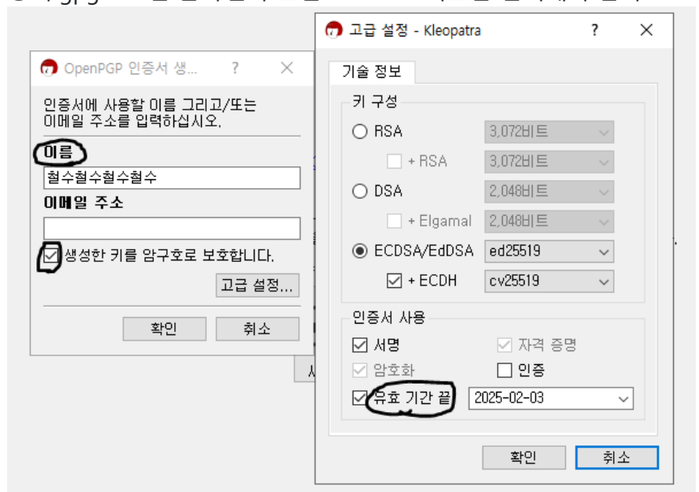
4.1.1.3. 키 생성하기

1. 철수: 파일 -> 새 키 쌍 클릭



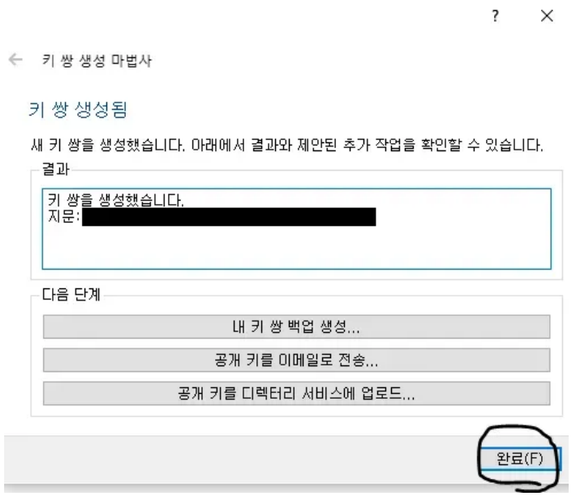
2. 철수: '개인 OpenPGP 키 쌍 생성' 클릭

3. 철수: 이름입력, '생성한 키를 암구호로 보호합니다' 선택, 유효 기간 적당하게 조절 후 생성한다.
키 구성은 ECDSA/EdDSA(ed25519)+ECDH(cv25519) (=기본 설정 그대로) 또는 RSA 4096비트(3072비트 아님)를 선택한다.
PGP 프로그램 중 gpg4usb가 있는데 이 프로그램은 ECDSA/EdDSA(ed25519)를 지원하지 않는다. 그러므로 만약 상대방이 gpg4usb를 쓴다면 무조건 RSA 4096비트를 선택해야 한다.



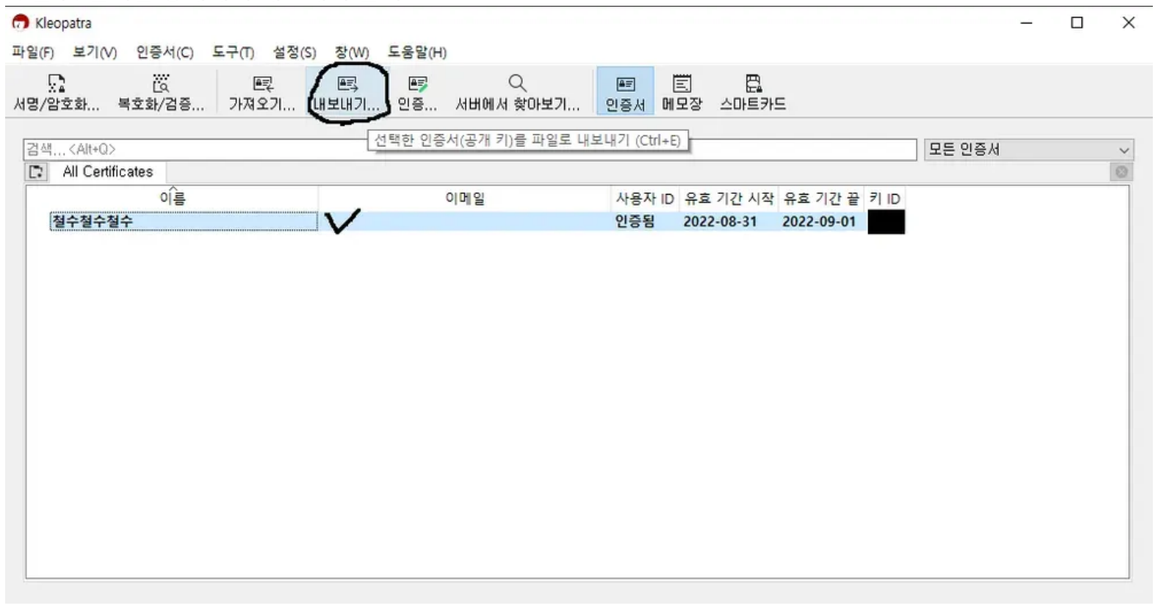
4. 철수: 비밀번호 입력

5. 철수: 완료 클릭

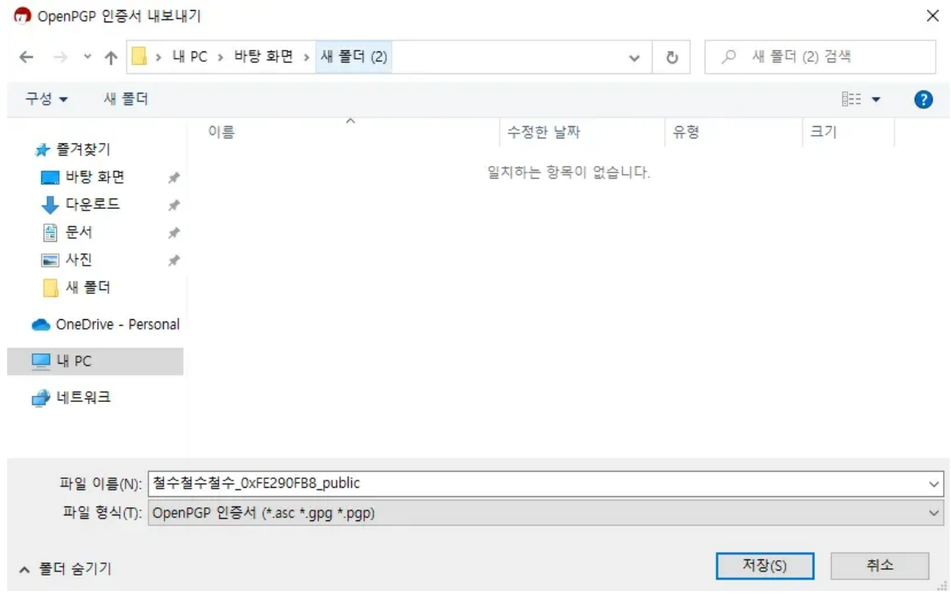


4.1.1.4. 내 공개키 내보내기

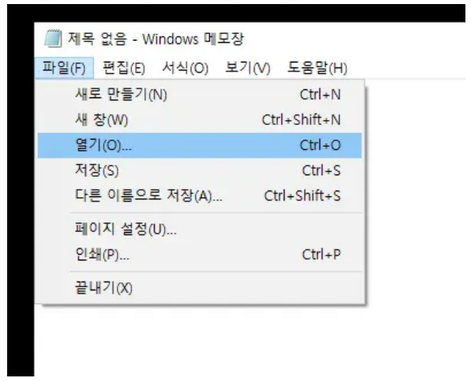
1. 철수: 선택한 상태에서 내보내기 클릭


Kleopatra
파일(F) 보기(V) 인증서(C) 도구(T) 설정(S) 창(W) 도움말(H)
서명/암호화... 복호화/검증... 가져오기... 내보내기... 인증... 서버에서 찾아보기... 인증서 메모장 스마트카드
선택한 인증서(공개 키)를 파일로 내보내기 (Ctrl+E)
검색... <Alt+Q>
모든 인증서
All Certificates
이름 이메일 사용자 ID 유효 기간 시작 유효 기간 끝 키 ID
철수철수철수 인증됨 2022-08-31 2022-09-01

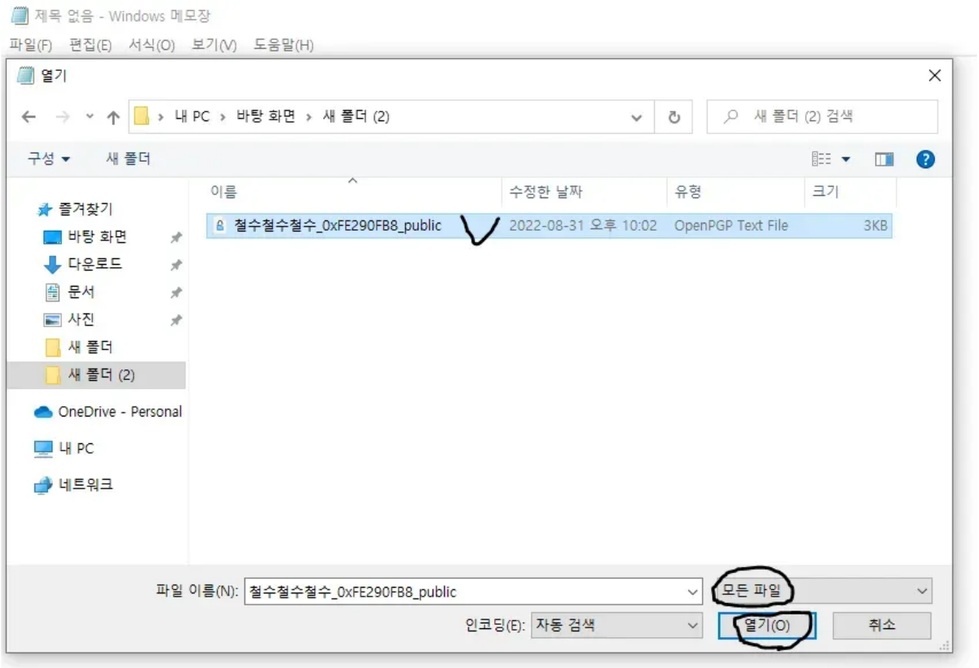
2. 철수: 저장



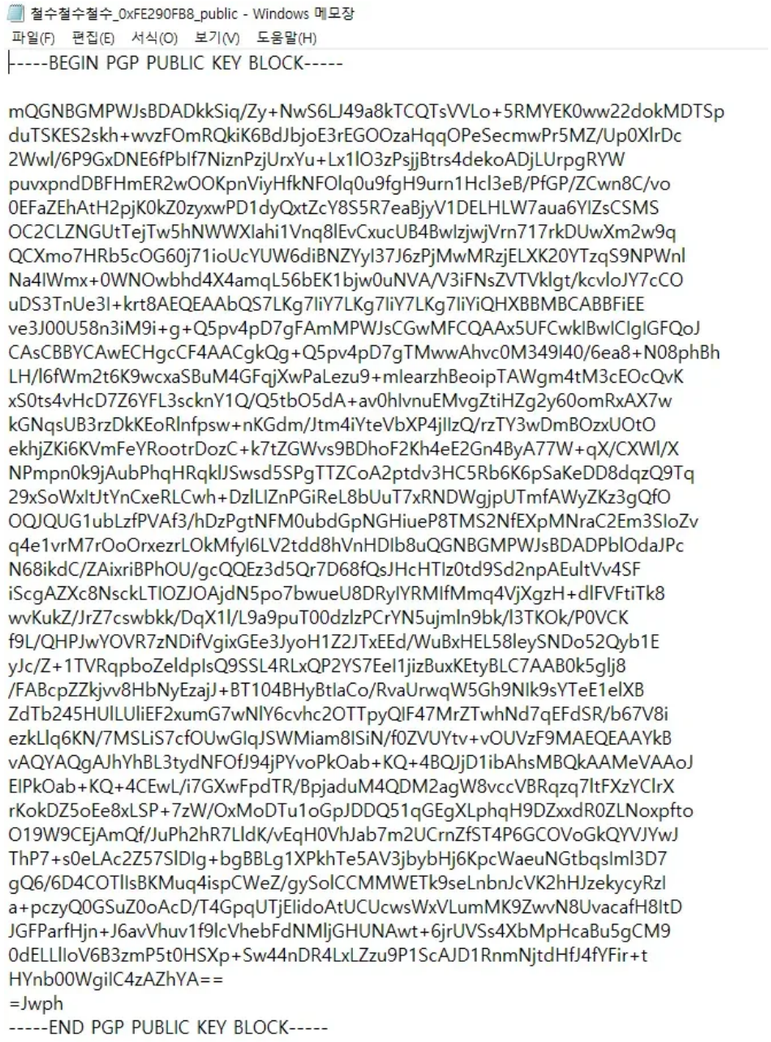
3. 철수: 메모장 -> 파일 -> 열기



4. 철수: 모든 파일로 변경 후 파일을 선택하고 열기 클릭



5. 철수: 자신(철수)의 공개키이다.



6. 철수: 전체선택(ctrl+a) 후 복사(ctrl+c)

철수철수철수_0xFE290FB8_public - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGMPWJsBDADkkSiq/Zy+NwS6LJ49a8kTCQTsVVLo+5RMYEK0ww22dokMDTSp
duTSKES2skh+wvzFOmRQkiK6BdJbjoE3rEGOOzaHqqOPeSecmwPr5MZ/Up0XlrDc
2Wwl/6P9GxDNE6fPbIf7NiznPzjUrxYu+Lx1lO3zPsjjBtrs4dekoADjLUrpgRYW
puvxpndDBFHmER2wOOKpnViyHfkNFOlq0u9fgH9urn1Hcl3eB/PfGP/ZCwn8C/vo
0EFaZEhAtH2pjK0kZ0zyxwPD1dyQxtZcY8S5R7eaBjyV1DELHLW7aua6YIZsCSMS
OC2CLZNGUtTejTw5hNWWXIahi1Vnq8lEvCxucUB4BwIzjwjVrn717rkDUwXm2w9q
QCXmo7HRb5cOG60j71ioUcYUW6diBNZYyI37J6zPjMwMRzjELXK20YTzqS9NPWnl
Na4lWmx+0WNOwbhd4X4amqL56bEK1bjw0uNVA/V3iFNsZVTVklgt/kcvloJY7cCO
uDS3TnUe3I+krt8AEQEAAbQS7LKg7IiY7LKg7IiY7LKg7IiYiQHXBBMBCABBFiEE
ve3J00U58n3iM9i+g+Q5pv4pD7gFAmMPWJsCGwMFCQAAx5UFCwklBwICIgIGFQoJ
CAsCBBYCAwECHgcCF4AACgkQg+Q5pv4pD7gTMwwAhvc0M349l40/6ea8+N08phBh
LH/l6fWm2t6K9wcxaSBuM4GFqjXwPaLezu9+mlearzhBeoipTAWgm4tM3cEOcQvK
xS0ts4vHcD7Z6YFL3scknY1Q/Q5tbO5dA+av0hlvnuEMvgZtiHZg2y60omRxAX7w
kGNqsUB3rzDkKEoRlnfpsw+nKGdm/Jtm4iYteVbXP4jIlzQ/rzTY3wDmBOzxUOtO
ekhjZKi6KVmFeYRootrDozC+k7tZGWvs9BDhoF2Kh4eE2Gn4ByA77W+qX/CXWl/X
NPmpn0k9jAubPhqHRqklJSwsd5SPgTTZCoA2ptdv3HC5Rb6K6pSaKeDD8dqzQ9Tq
29xSoWxltJtYnCxeRLCwh+DzlLIZnPGiReL8bUuT7xRNDWgjpUTmfAWyZKz3gQfO
OQJQUG1ubLzfPVAf3/hDzPgtNFM0ubdGpNGHiueP8TMS2NfEXpMNraC2Em3SIoZv
q4e1vrM7rOoOrxezrLOkMfyI6LV2tdd8hVnHDIb8uQGNBGMPWJsBDADPblOdaJPc
N68ikdC/ZAixriBPhOU/gcQQEz3d5Qr7D68fQsJHcHTlz0td9Sd2npAEultVv4SF
iScgAZXc8NsckLTIOZJOAjdN5po7bwueU8DRyIYRMIfMmq4VjXgzH+dlFVFtiTk8
wvKukZ/JrZ7cswbkk/DqX1l/L9a9puT00dzlzPCrYN5ujmln9bk/l3TKOk/P0VCK
f9L/QHPJwYOVR7zNDifVgixGEe3JyoH1Z2JTxEEd/WuBxHEL58leySNDo52Qyb1E
yJc/Z+1TVRqpboZeldpIsQ9SSL4RLxQP2YS7EeI1jizBuxKEtyBLC7AAB0k5glj8
/FABcpZZkjvv8HbNyEzajJ+BT104BHyBtlaCo/RvaUrwqW5Gh9Nlk9sYTeE1elXB
ZdTb245HUlLUliEF2xumG7wNlY6cvhc2OTTpyQIF47MrZTwhNd7qEFdSR/b67V8i
ezkLlq6KN/7MSLiS7cfOUwGlqJSWMiam8lSiN/f0ZVUYtv+vOUVzF9MAEQEAAYkB
vAQYAQgAJhYhBL3tydNFOfJ94jPYvoPkOab+KQ+4BQJjD1ibAhsMBQkAAMeVAAoJ
ElPkOab+KQ+4CEwL/i7GXwFpdTR/BpjaduM4QDM2agW8vccVBRqzq7ltFXzYClrX
rKokDZ5oEe8xLSP+7zW/OxMoDTu1oGpJDDQ51qGEgXLphqH9DZxxdR0ZLNoxpfto
O19W9CEjAmQf/JuPh2hR7LldK/vEqH0VhJab7m2UCrnZfST4P6GCOVoGkQYVJYwJ
ThP7+s0eLAc2Z57SlDlg+bgBBLg1XPkhTe5AV3jbybHj6KpcWaeuNGtbqsIml3D7
gQ6/6D4COTllsBKMuq4ispCWeZ/gySolCCMMWETk9seLnbnJcVK2hHJzekycyRzl
a+pczyQ0GSuZ0oAcD/T4GpqUTjElidoAtUCUcwsWxVLumMK9ZwvN8UvacafH8ltD
JGFParfHjn+J6avVhuv1f9lcVhebFdNMljGHUNAwt+6jrUVSs4XbMpHcaBu5gCM9
0dELLlloV6B3zmP5t0HSXp+Sw44nDR4LxLZzu9P1ScAJD1RnmNjtdHfJ4fYFir+t
HYnb00WgilC4zAZhYA==
=Jwph
-----END PGP PUBLIC KEY BLOCK-----

7. 철수: 자신의 프로필에 공개키 붙여넣기 (아카는 공개키를 넣을 수 있는 프로필 공간이 없어서 임시로 아래와 같이 했음)

GPG연습) 철수의 프로필

철수 추천 0 | 비추

아래는 철수의 공개키입니다

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGMPWJsBDADkkSiq/Zy+NwS6LJ49a8kTCQTsVVLo+5RMYEK0ww22dokMDTSp
duTSKES2skh+wvzFOmRQkiK6BdJbjoE3rEGOOzaHqqOPeSecmwPr5MZ/Up0XlrDc
2Wwl/6P9GxDNE6fPbIf7NiznPzjUrxYu+Lx1lO3zPsjjBtrs4dekoADjLUrpgRYW
puvxpndDBFHmER2wOOKpnViyHfkNFOlq0u9fgH9urn1Hcl3eB/PfGP/ZCwn8C/vo
0EFaZEhAtH2pjK0kZ0zyxwPD1dyQxtZcY8S5R7eaBjyV1DELHLW7aua6YIZsCSMS
OC2CLZNGUtTejTw5hNWWXIahi1Vnq8lEvCxucUB4BwIzjwjVrn717rkDUwXm2w9q
QCXmo7HRb5cOG60j71ioUcYUW6diBNZYyI37J6zPjMwMRzjELXK20YTzqS9NPWnl
Na4lWmx+0WNOwbhd4X4amqL56bEK1bjw0uNVA/V3iFNsZVTVklgt/kcvloJY7cCO
uDS3TnUe3I+krt8AEQEAAbQS7LKg7IiY7LKg7IiY7LKg7IiYiQHXBBMBCABBFiEE
ve3J00U58n3iM9i+g+Q5pv4pD7gFAmMPWJsCGwMFCQAAx5UFCwklBwICIgIGFQoJ
CAsCBBYCAwECHgcCF4AACgkQg+Q5pv4pD7gTMwwAhvc0M349l40/6ea8+N08phBh
LH/l6fWm2t6K9wcxaSBuM4GFqjXwPaLezu9+mlearzhBeoipTAWgm4tM3cEOcQvK
xS0ts4vHcD7Z6YFL3scknY1Q/Q5tbO5dA+av0hlvnuEMvgZtiHZg2y60omRxAX7w
kGNqsUB3rzDkKEoRlnfpsw+nKGdm/Jtm4iYteVbXP4jIlzQ/rzTY3wDmBOzxUOtO
ekhjZKi6KVmFeYRootrDozC+k7tZGWvs9BDhoF2Kh4eE2Gn4ByA77W+qX/CXWl/X
NPmpn0k9jAubPhqHRqklJSwsd5SPgTTZCoA2ptdv3HC5Rb6K6pSaKeDD8dqzQ9Tq
29xSoWxltJtYnCxeRLCwh+DzlLIZnPGiReL8bUuT7xRNDWgjpUTmfAWyZKz3gQfO
OQJQUG1ubLzfPVAf3/hDzPgtNFM0ubdGpNGHiueP8TMS2NfEXpMNraC2Em3SIoZv
q4e1vrM7rOoOrxezrLOkMfyI6LV2tdd8hVnHDIb8uQGNBGMPWJsBDADPblOdaJPc
N68ikdC/ZAixriBPhOU/gcQQEz3d5Qr7D68fQsJHcHTlz0td9Sd2npAEultVv4SF
iScgAZXc8NsckLTIOZJOAjdN5po7bwueU8DRyIYRMIfMmq4VjXgzH+dlFVFtiTk8
wvKukZ/JrZ7cswbkk/DqX1l/L9a9puT00dzlzPCrYN5ujmln9bk/l3TKOk/P0VCK
f9L/QHPJwYOVR7zNDifVgixGEe3JyoH1Z2JTxEEd/WuBxHEL58leySNDo52Qyb1E
yJc/Z+1TVRqpboZeldpIsQ9SSL4RLxQP2YS7EeI1jizBuxKEtyBLC7AAB0k5glj8
/FABcpZZkjvv8HbNyEzajJ+BT104BHyBtlaCo/RvaUrwqW5Gh9Nlk9sYTeE1elXB
ZdTb245HUlLUliEF2xumG7wNlY6cvhc2OTTpyQIF47MrZTwhNd7qEFdSR/b67V8i
ezkLlq6KN/7MSLiS7cfOUwGlqJSWMiam8lSiN/f0ZVUYtv+vOUVzF9MAEQEAAYkB
vAQYAQgAJhYhBL3tydNFOfJ94jPYvoPkOab+KQ+4BQJjD1ibAhsMBQkAAMeVAAoJ
ElPkOab+KQ+4CEwL/i7GXwFpdTR/BpjaduM4QDM2agW8vccVBRqzq7ltFXzYClrX

rKokDZ5oEe8xLSP+7zW/OxMoDTu1oGpJDDQ51qGEgXLphqH9DZxxdR0ZLNoxpfto
O19W9CEjAmQf/JuPh2hR7LldK/vEqH0VhJab7m2UCrnZfST4P6GCOVoGkQYVJYwJ
ThP7+s0eLAc2Z57SlDlg+bgBBLg1XPkhTe5AV3jbybHj6KpcWaeuNGtbqsIml3D7
gQ6/6D4COTlIsBKMuq4ispCWeZ/gySolCCMMWETk9seLnbnJcVK2hHJzekycyRzI
a+pczyQ0GSuZ0oAcD/T4GpqUTjEIidoAtUCUcwsWxVLumMK9ZwvN8UvacafH8ltD
JGFParfHjn+J6avVhuv1f9lcVhebFdNMljGHUNAwt+6jrUVSs4XbMpHcaBu5gCM9
0dELLlIoV6B3zmP5t0HSXp+Sw44nDR4LxLZzu9P1ScAJD1RnmNjtdHfJ4fYFir+t
HYnb00WgiIC4zAZhYA==
=Jwph
-----END PGP PUBLIC KEY BLOCK-----

영희도 철수와 동일한 과정을 거친다.

4.1.1.5. 상대방 공개키 들여오기

1. 철수: 영희의 공개키를 복사

GPG연습) 영희의 프로필

영희 추천 0 | 비추천 0

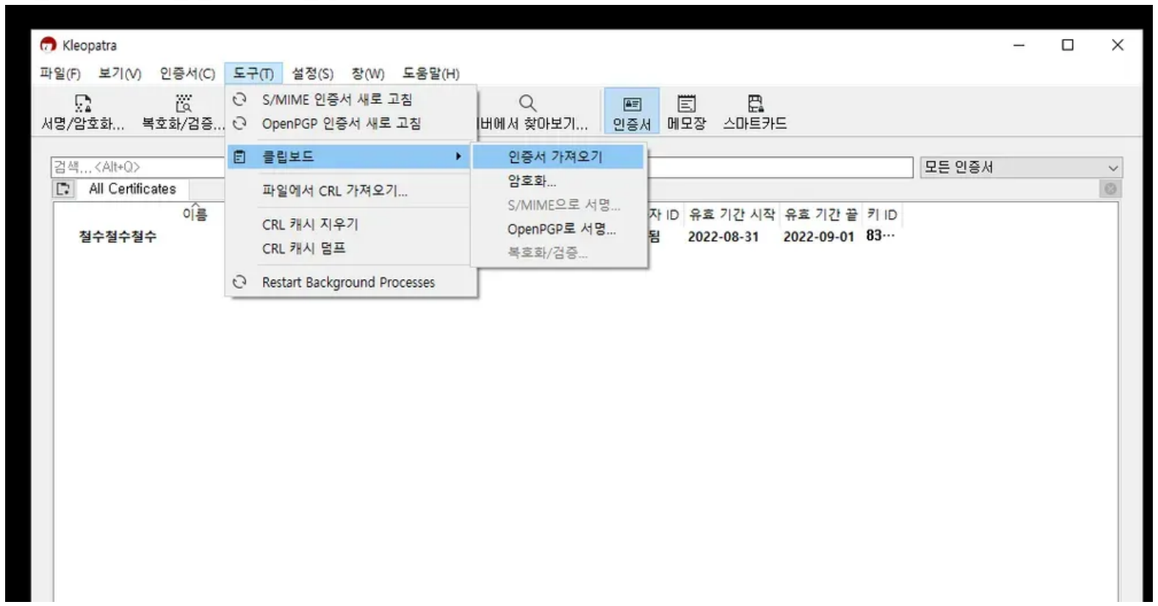
아래는 영희의 공개키입니다

-----BEGIN PGP PUBLIC KEY BLOCK-----

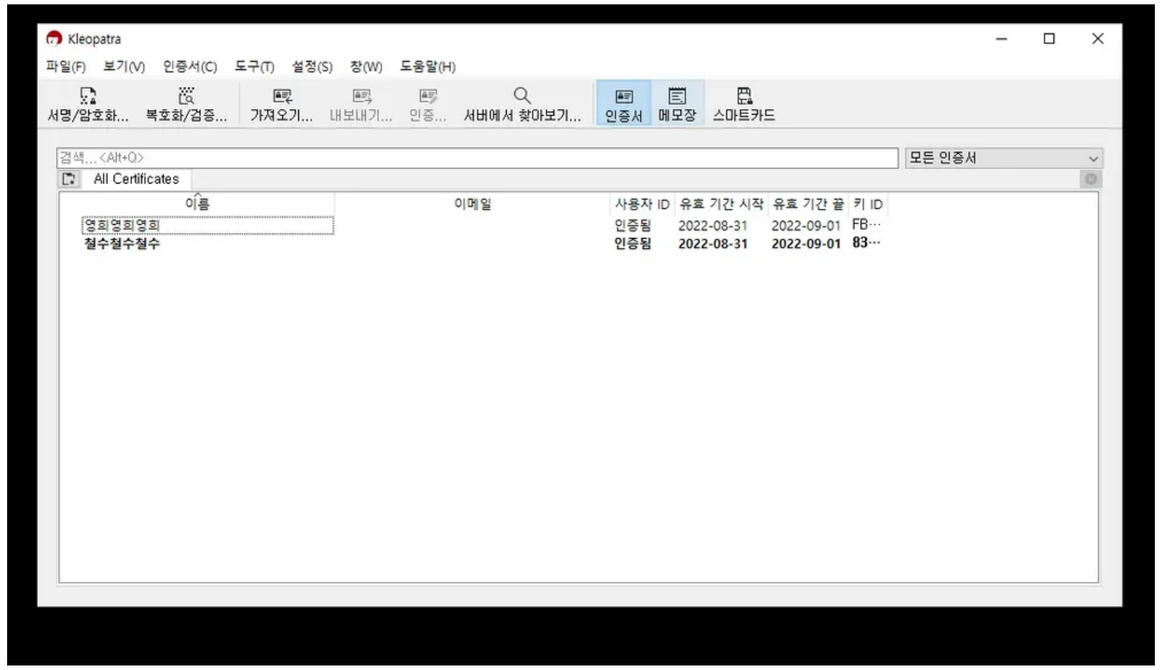
mQGNBGMPYLMBDADUESwxKMKlHmpPlOZ67rVLkiKDYu1jkCD6nbrDLnoZIqcBmv2B
dTB7BDreKdWJ98yt6xUv3TLGXG9Xx8SY/asLtc8Bs6+NAZ5G0XPeMXlNoXs97xyf
lbH+se6c04LE+2fapWSG3A1s1poL4cnHTPaD0Ftj/cSvYTHSDDXGHigY8p5VzEFL
BrjzhfDagsStRgrRjZz+WeYHgsfSmLk+65Kajli7ry8qfGs10dfg5p1lQd35smzy
B7QVy6y50pUDQ+aREGugmuCUpypcXrbFkm5XvabC5nb+JvGNKsH7PmK0sJRqCFYe
/FLmxTJZQOMcJOglqlogkoXBwPzSfvtLUgDNQJQqC6LbhIlcx04KUIO9Ncelw30X
IJueilNyEdYugJQw+pk6cMbzxgjfN6oI+ix7vwXqcKg4UCNHGSl9QKqb7hhKNC0n
oTMuGSGDzLff5vf8TDkcnxEFo/K7gFbLmEAIob3lQgz42vg5qHsJ92uPdSg5clwI
tv9S6hqWDI5IP6UAEQEAAbQS7JiB7Z2s7JiB7Z2s7JiB7Z2siQHXBBMBCABBFiEE
R+ZpehtPJuJcusIJ+11o2fTFSToFAmMPYLMCGwMFCQAAv30FCwkIBwICIgIGFQoJ
CAsCBBYCAwECHgcF4AACgkQ+11o2fTFSTop1QwAwco7/pCBmhgSQbN+7P4QNm6X
sCahyUvaP0Lxb54+bQ+wC7sz5TKT6FN1n00cW1YcVjKd0qxHPXu+N63UUtd83G20
41dhpvLlnD+iAFCdN0lL2iD+Lh7oGABcDabzvlw7fG4Zy9wJomZcRZz82w638fJC
zBek7i0xMbm4K4jQXfNd8bm2tCKL+FQRF+wRGnpvQE1aos2CWKoQrYcP0e7KjLGe
2WTIIL3qolK/K7iHBtuy5gk6E/uHbZBMGZ8RfssB2BaSqYJUVuZJauAhHAXcpLIb
+koIRwGaMKguRwiBSZ4lzNBjcaVZ6WnRaJNOSRIIB/pklAnP1AAkCILU2fSg0G68
hXzooDxagfH1/ENRA7bjmQUxxnZDaq3nFmK3qMdubbSVMd78oHJJseExg9igu/dT
bnkcS/ntPsTV39yXIAKWZ8TCENcFPsINJpcni2/hupCVDvW2lHaBUUulkgKXPCUT
TvrxlvmQGUG02uUW9STWB/SyYFD+GKEQPBiNPBhzuQGNBGMPYLMBDAC30VT2RDYi
3FSdnzTcQ+X8YS1E+aDu9P0Gq9uuPRSZOfRAYVKC0ub04b/9IOG2Tmh7I0IKGMqt
Mf3JU5VwQO+5gz9eXYTFO2bBfrnIL9D3/kqQx52fAhKzfo3PoXUmS0Xzmvx2aKDG
nMI5a9fFiVPSF7JILyCcVQoOoPjsotgaiqf0Dnqce4re8pRaQRNP1xHP+ZPH2seL
R2BzW5t86I8KkBPvBYYPItydsIuKR6SoVeZuVTHJpB/mMxWbJKWFRnlZ4pAL/qTh
srZowU6YshutClTd6eOKRBgoXvYYsVbuYhTeMNFOQf8G22t13k/+coQZRisSJk3L
E87J1nIDnJS2zDomx2SOSRdJElZjSEuSZEehW5aumI7zbfBdKt2kQDNGVf7T8moY
RGW04fbD7mJS/1NHBSm8zyFZB528J4Sxy7r1AkhS41AzqBibPrrTtdbblG93Tknf
JXth0zv1HcyVXj+UyYGTjttcSQfAHP1harX/L7sCOFiSK4OjD5ddH00AEQEAAYkB
vAQYAQgAJhYhBEfmaXobTybiXLrCCftdaNn0xUk6BQJjD2CzAhsMBQkAAL99AAoJ
EPtdaNn0xUk6jSIL+gLFxTwaxnLKGWUXC0wUHclNPmF7rxrDUn1VvENyGb4QMGpo

1cyQ56619WfzFrEnuxU1KWVjgQzhbbWkd8QNJQgO92W/fLPUQGH1AHs8C+QcjTXB
oJOp24epsLUrMyjzV9XkDsDj7vRLTIMtWgENOgEI/shwKAHrzv9B6uRwy8Iq1FJu
Jbib8agf3ArmO7QiUX1Z5eG+qSEdfcVwhIJG9ZSTXe71+OKX3nP6WFqRcG/bKqz5
InyfdcziMV9GCjuoCRIfe730ITZ8N8+dFt8RsfmTCuNRxeh5q0A7J7rIFeXAZhmH
prsCP6emb1XCH74GlnOPr4M4BP4AhqL9m5Mo225BICU5Yo7A599AcsycAsCl/2M3
UDohImWLA/k1as0iGkFQpp52xxZV3h9MpLJYR43l6u7NSsBbdDgtmEfOAXhIWKF4
ZbRVr1AJbIvYhDJJgYPByFSMe73VeD6S/17ou2gT2e/zXgxALTV2CsyTpYb8ZIJP
0Yq/VBC16vZTyAkODA==
=g0Oq
-----END PGP PUBLIC KEY BLOCK-----

2. 철수: 도구 -> 클립보드 -> 인증서 가져오기



3. 철수: 영희를 추가한다.

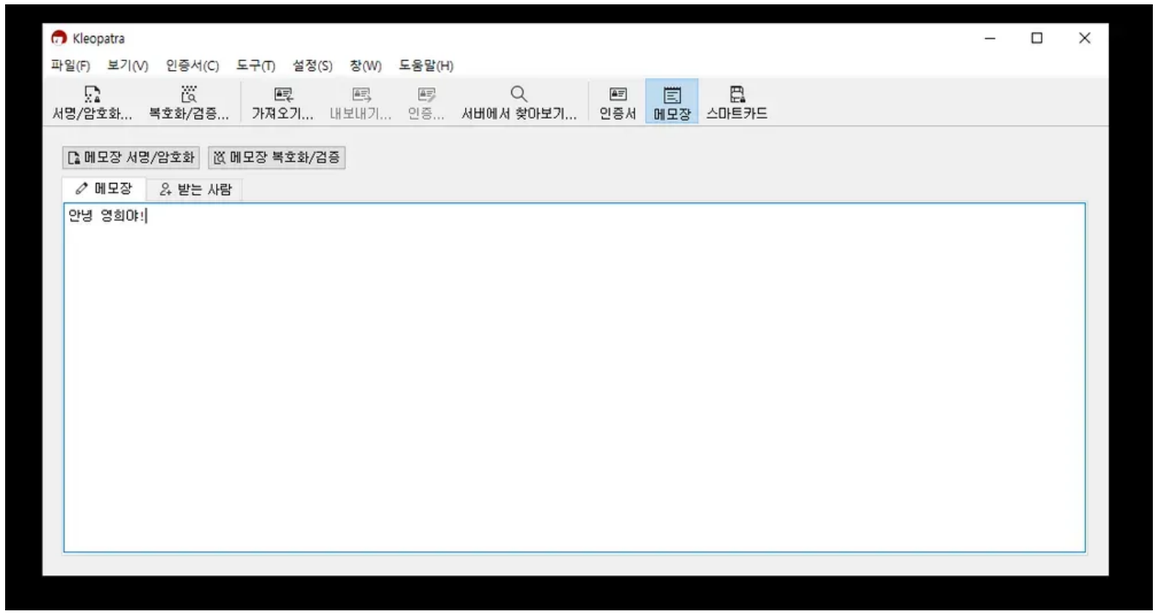


영희도 철수와 동일한 과정을 거친다.

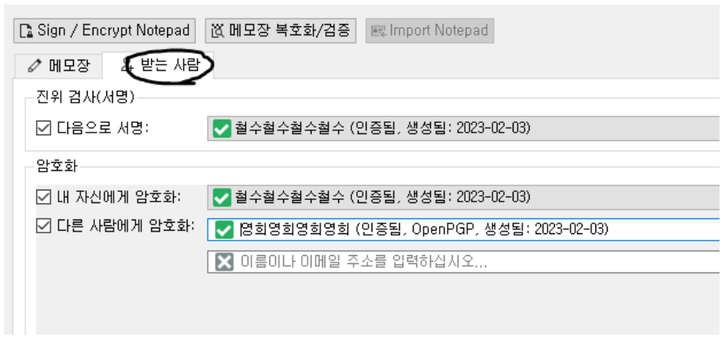
4.1.1.6. 암호문 보내기

1. 철수: 클레오파트라에서 메모장 클릭

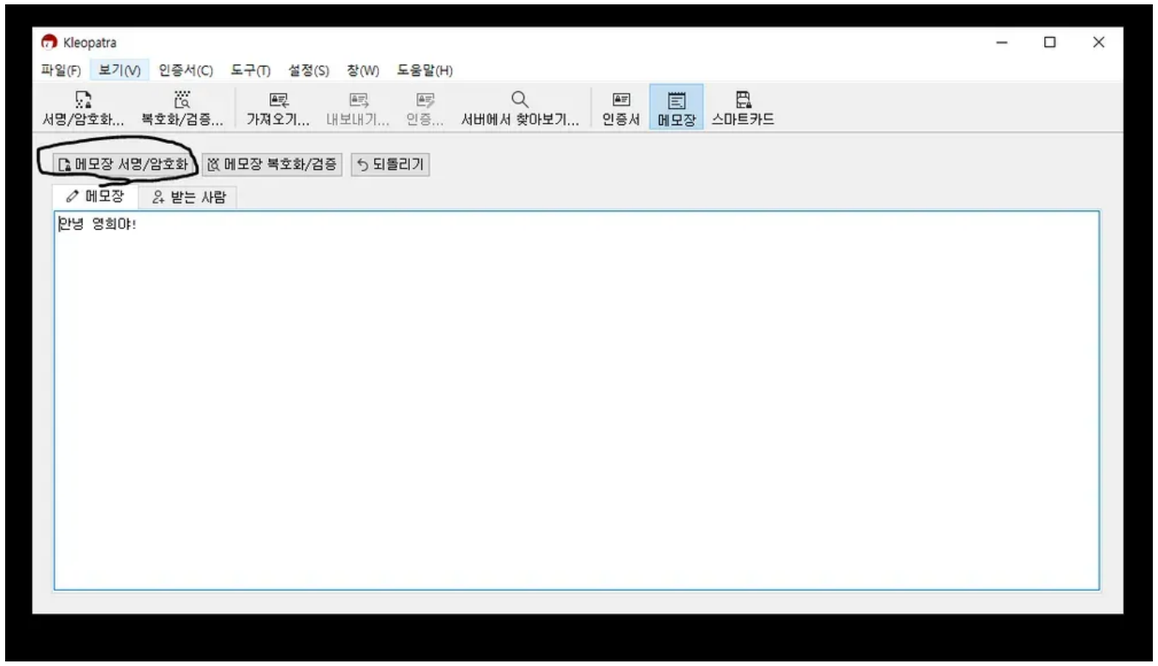
2. 철수: 메세지 입력



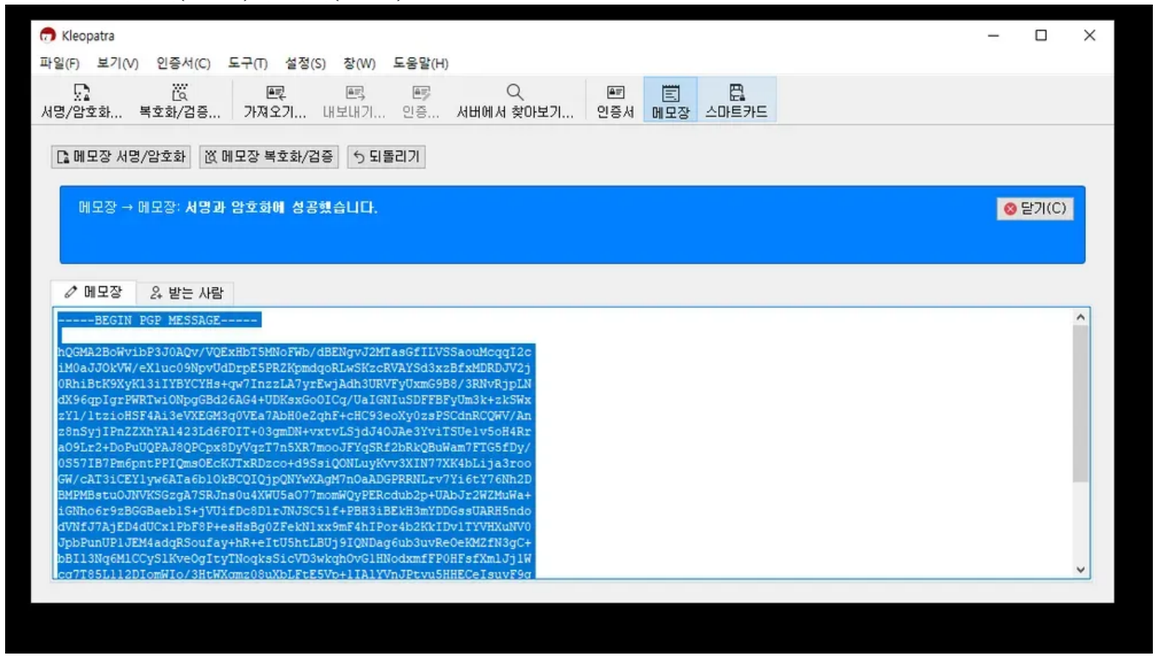
3. 철수: 받는 사람 탭에서 아래와 같이 설정한다.



4. 철수: 메모장 서명/암호화 클릭



5. 철수: 전체선택(ctrl+a) 후 복사(ctrl+c)



6. 철수: 게시글 작성

영희 2022-08-31 22:41:42 | 신고 | 답글

알았어~

댓글 작성 철수 음성댓글 아카론

-----BEGIN PGP MESSAGE-----

hQGMA2BoWvibP3J0AQv/VQExHbT5MNoFWb/dBENgvJ2MTasGfILVSSaouMcqqI2c
iM0aJJOkVW/eX1uc09NpvUdDrpE5PRZKpmdqoRLwSKzcRVAYSd3xzBfxMDRDJV2j
0RhiBtK9XyKl3iIYBYCYHs+qw7InzzLA7yrEwjAdh3URVFyUxmG9B8/3RNvRjpLN
dX96qpIgrPWRTwiONpgGBd26AG4+UDKsxGoOICq/UaIGNIuSDFFBFyUm3k+zkSWx
zYl/1tzioHSF4Ai3eVXEGM3q0VEa7AbH0eZqhF+cHC93eoXy0zsPSCdnRCQWV/An
z8nSyjIPnZZXhYAI423Ld6FOIT+03gmDN+vxtvLSjdJ4OJAe3YviTSUe1v5oH4Rr
aO9Lr2+DoPuUQPAJ8QPCpx8DyVqzT7n5XR7mooJFYqSRf2bRkQBuWam7FTG5fDy/
0S57IB7Pm6pntPPIQmsOEcKJTxRDzco+d9SsiQONLuyKvv3XIN77XK4bLija3roo
GW/cAT3iCEY1yw6ATa6b1OkBCQIQjpQNYwXAgM7nOaADGPRRNLrv7Yi6tY76Nh2D
BMPMBstuOJNVKSGzgA7SRJns0u4XWU5aO77momWQyPERcdub2p+UAbJr2WZMuWa+
iGNho6r9zBGGBaeb1S+jVUifDc8DlrJNJSC51f+PBH3iBEkH3mYDDGssUARH5ndo
dVNfJ7AjED4dUCxlPbF8P+esHsBg0ZFekNlxx9mF4hIPor4b2KkIDv1TYVHXuNV0
JpbPunUP1JEM4adqRSoufay+hR+eItU5htLBUj9IQNDag6ub3uvReOeKMZfN3gC+
bBII3Nq6MlCCySlKveOgItyTNoqksSicVD3wkqhOvG1HNodxmfFP0HFsfXmlJj1W
cq7T85L112DIomWIo/3HtWXqmz08uXbLFtE5Vp+1IAlYVnJPtyu5HHECeIsuyF9g
DrFQ+g8h98TOzn0OJ/0in42+/4QSXx3lgeUjgwlbke8IKaJtFAQ7KdckSfNZoBU0
5R3tdpQ/+NduF5rXu7XdS+nulyWRdGbGrK/subfg89Ll/PaUW9oEF35XCltaoxfU
tzvVkAcJfZmjA3UGPl4lqfW1iSKrJjPu6MxS4Ff2ev9enkJCMeOeXtP1gn/dZuxt
ykigsBNadCVVHlyJE4Fwyb3gWE5CALMShBlEem0Bfie4USIuogFjOovS+F3P926J
6x4RDb9M4hESvwZPL8fc3gSSP6jDtp9MAQSRHZ7XBYE=
=j95Q
-----END PGP MESSAGE-----

7. 영희: 철수의 암호문을 복사한다

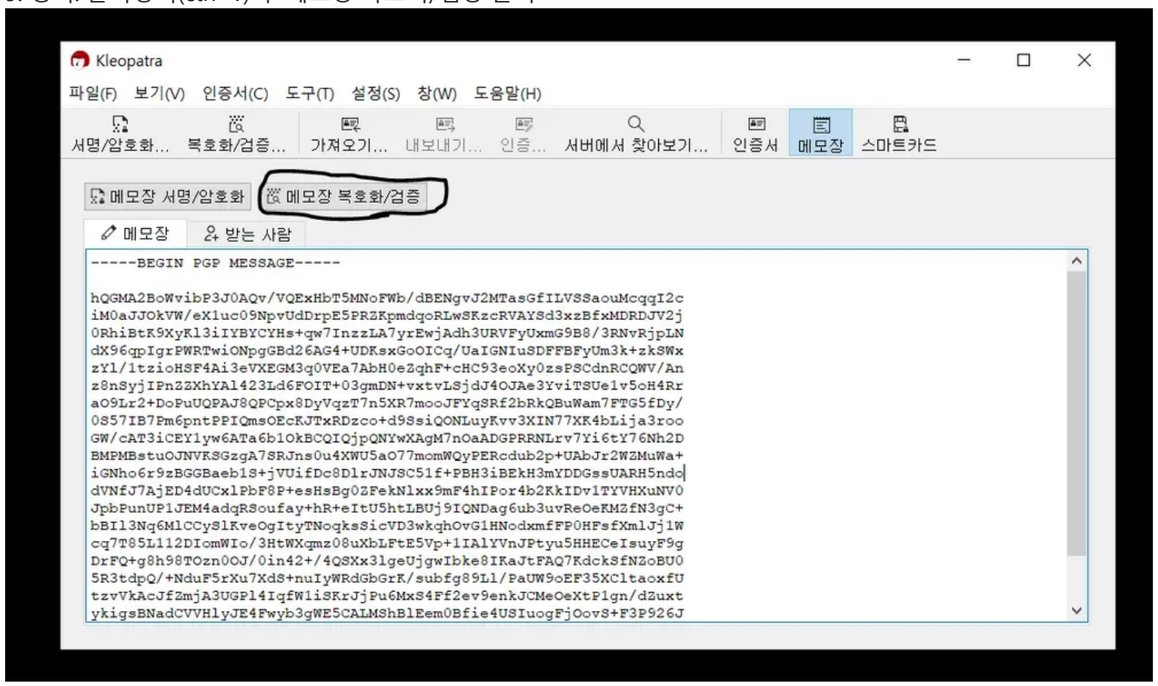
철수 2022-08-31 23:22:54 | 신고 | 답글

-----BEGIN PGP MESSAGE-----

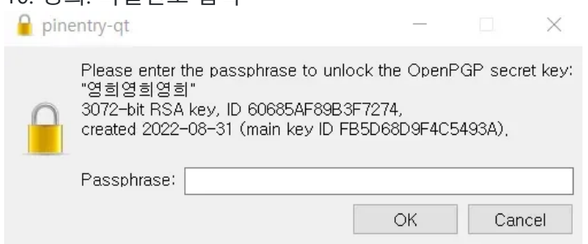
hQGMA2BoWvibP3J0AQv/VQExHbT5MNoFWb/dBENgvJ2MTasGfILVSSaouMcqqI2c
iM0aJJOkVW/eX1uc09NpvUdDrpE5PRZKpmdqoRLwSKzcRVAYSd3xzBfxMDRDJV2j
0RhiBtK9XyKl3iIYBYCYHs+qw7InzzLA7yrEwjAdh3URVFyUxmG9B8/3RNvRjpLN
dX96qpIgrPWRTwiONpgGBd26AG4+UDKsxGoOICq/UaIGNIuSDFFBFyUm3k+zkSWx
zYl/1tzioHSF4Ai3eVXEGM3q0VEa7AbH0eZqhF+cHC93eoXy0zsPSCdnRCQWV/An
z8nSyjIPnZZXhYAI423Ld6FOIT+03gmDN+vxtvLSjdJ4OJAe3YviTSUe1v5oH4Rr
aO9Lr2+DoPuUQPAJ8QPCpx8DyVqzT7n5XR7mooJFYqSRf2bRkQBuWam7FTG5fDy/
0S57IB7Pm6pntPPIQmsOEcKJTxRDzco+d9SsiQONLuyKvv3XIN77XK4bLija3roo
GW/cAT3iCEY1yw6ATa6b1OkBCQIQjpQNYwXAgM7nOaADGPRRNLrv7Yi6tY76Nh2D
BMPMBstuOJNVKSGzgA7SRJns0u4XWU5aO77momWQyPERcdub2p+UAbJr2WZMuWa+
iGNho6r9zBGGBaeb1S+jVUifDc8DlrJNJSC51f+PBH3iBEkH3mYDDGssUARH5ndo
dVNfJ7AjED4dUCxlPbF8P+esHsBg0ZFekNlxx9mF4hIPor4b2KkIDv1TYVHXuNV0
JpbPunUP1JEM4adqRSoufay+hR+eItU5htLBUj9IQNDag6ub3uvReOeKMZfN3gC+
bBII3Nq6MlCCySlKveOgItyTNoqksSicVD3wkqhOvG1HNodxmfFP0HFsfXmlJj1W
cq7T85L112DIomWIo/3HtWXqmz08uXbLFtE5Vp+1IAlYVnJPtyu5HHECeIsuyF9g
DrFQ+g8h98TOzn0OJ/0in42+/4QSXx3lgeUjgwlbke8IKaJtFAQ7KdckSfNZoBU0
5R3tdpQ/+NduF5rXu7XdS+nulyWRdGbGrK/subfg89Ll/PaUW9oEF35XCltaoxfU
tzvVkAcJfZmjA3UGPl4lqfW1iSKrJjPu6MxS4Ff2ev9enkJCMeOeXtP1gn/dZuxt
ykigsBNadCVVHlyJE4Fwyb3gWE5CALMShBlEem0Bfie4USIuogFjOovS+F3P926J
6x4RDb9M4hESvwZPL8fc3gSSP6jDtp9MAQSRHZ7XBYE=
=j95Q
-----END PGP MESSAGE-----

8. 영희: 클레오파트라에서 메모장 클릭

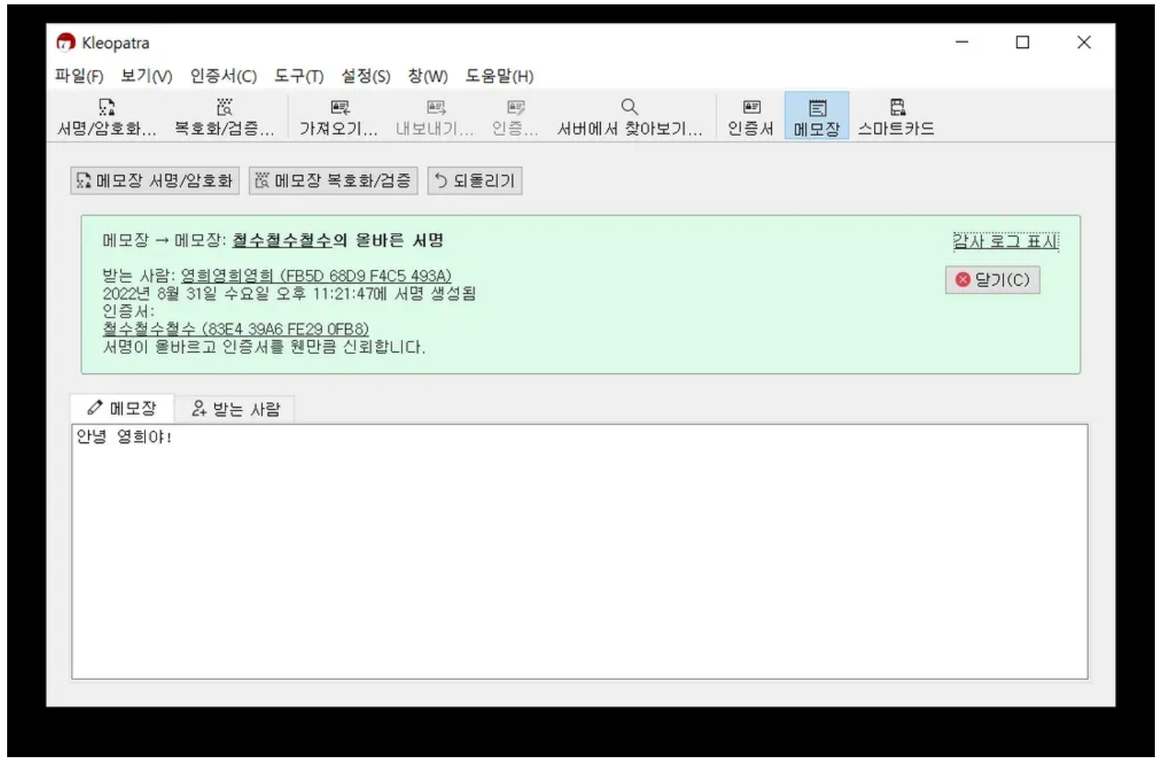
9. 영희: 붙여넣기(ctrl+v) 후 메모장 복호화/검증 클릭



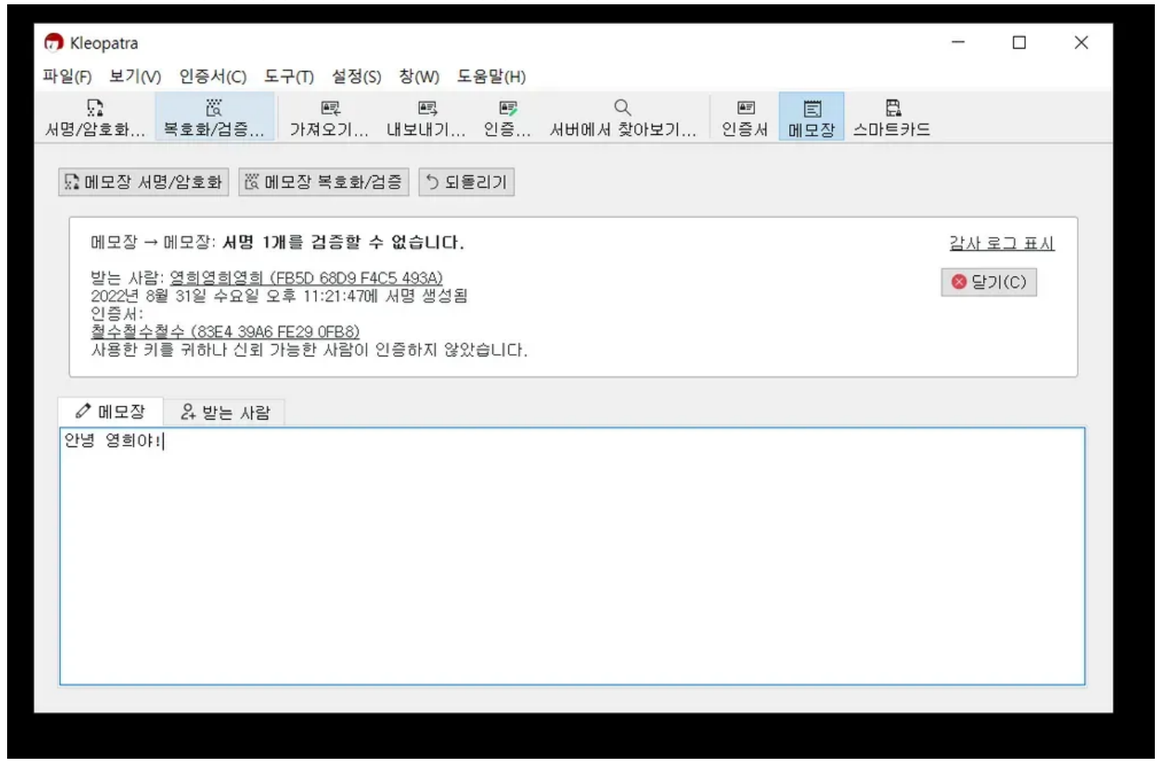
10. 영희: 비밀번호 입력



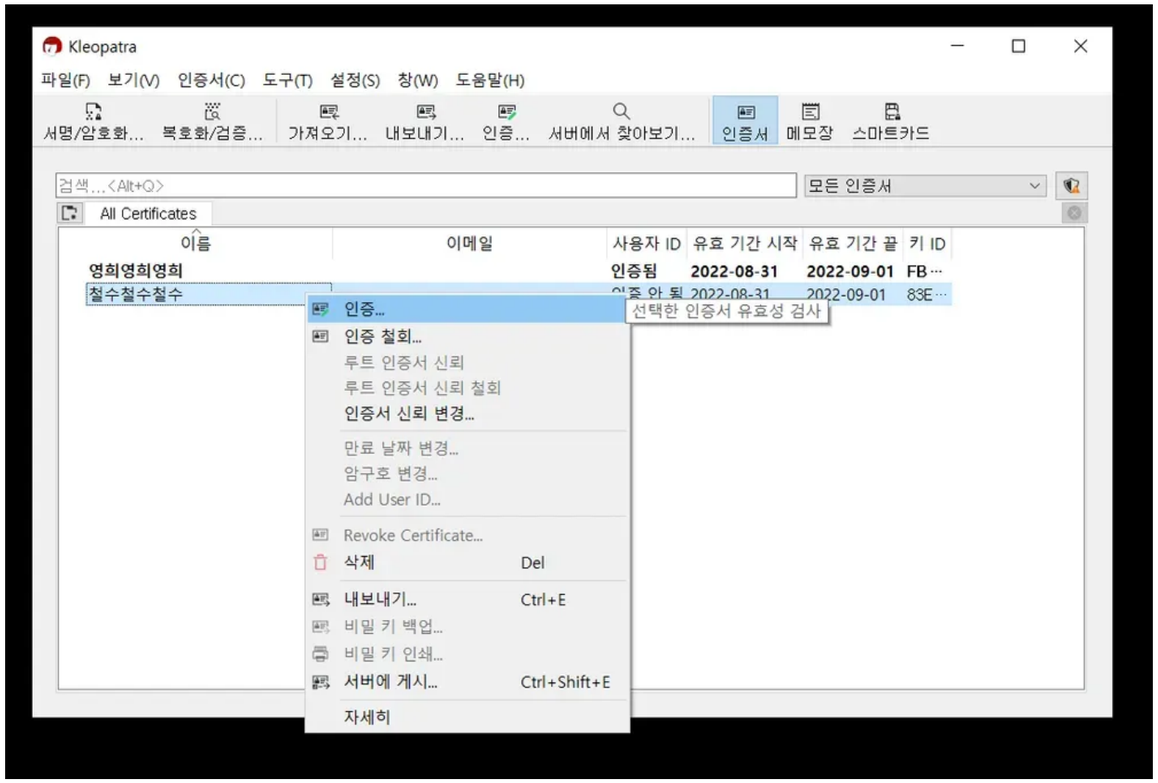
11. 영희: 결과1: 철수의 키가 '인증됨'으로 되어 있을 때



12. 영희: 결과2: 철수의 키가 '인증 안 됨'으로 되어 있을 때

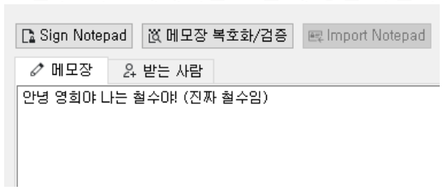

Kleopatra
파일(F) 보기(V) 인증서(C) 도구(T) 설정(S) 창(W) 도움말(H)
서명/암호화... 복호화/검증... 가져오기... 내보내기... 인증... 서버에서 찾아보기... 인증서 메모장 스마트카드
메모장 서명/암호화
메모장 복호화/검증
되돌리기
메모장 → 메모장: 서명 1개를 검증할 수 없습니다.
감사 로그 표시
받는 사람: 영희영희영희 (FB5D 68D9 F4C5 493A)
2022년 8월 31일 수요일 오후 11:21:47에 서명 생성됨
인증서:
철수철수철수 (83E4 39A6 FE29 0FB8)
사용한 키를 귀하나 신뢰 가능한 사람이 인증하지 않았습니다.
닫기(C)
메모장
받는 사람
안녕 영희야!

13. 영희: 우클릭해서 '인증 안 됨' -> '인증됨' 또는 '인증됨' -> '인증 안 됨' 으로 바꿔줄 수 있다.

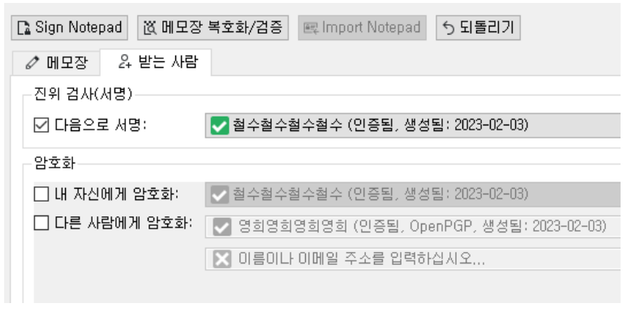


4.1.1.7. 메시지 서명하기

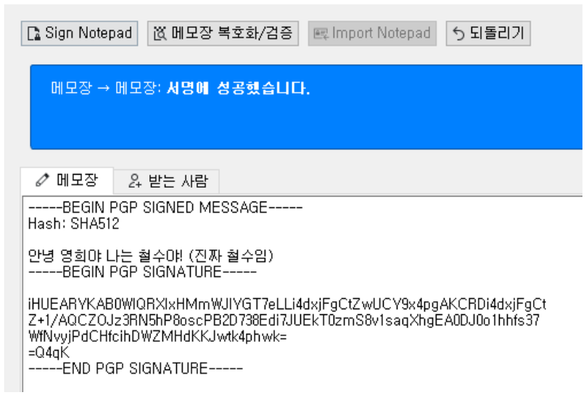
1. 철수: 서로 메세지를 보낼 때 정말 자신이 맞다는 것을 인증할 수도 있다. 먼저 메시지를 입력한다.



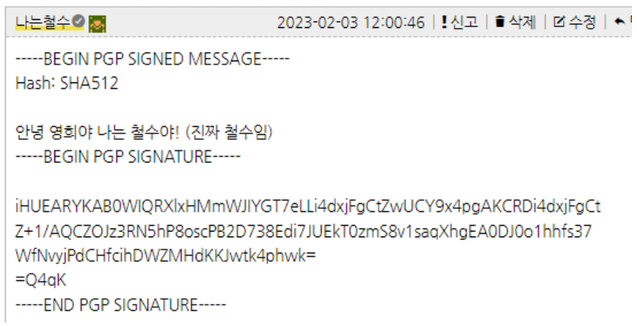
2. 철수: 받는 사람 클릭하고 아래 이미지와 같이 설정한다.



3. 철수: Sign Notepad 클릭

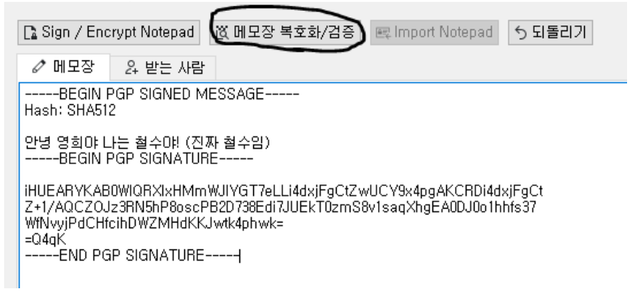


4. 철수: 게시판에 메시지를 올린다.

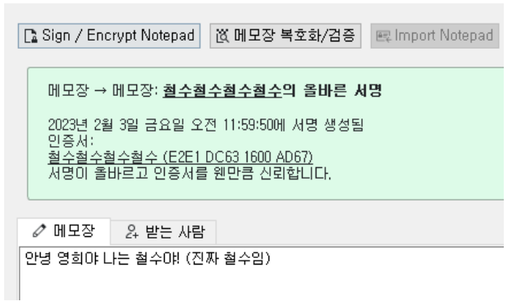


5. 영희: 철수의 메시지를 복사한다.

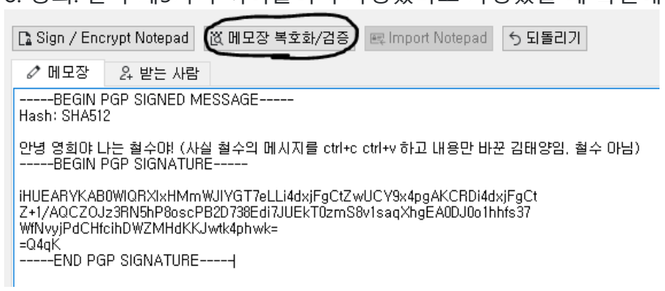
6. 영희: kleopatra의 메모장에 붙어넣은 뒤 메모장 복호화/검증 클릭.



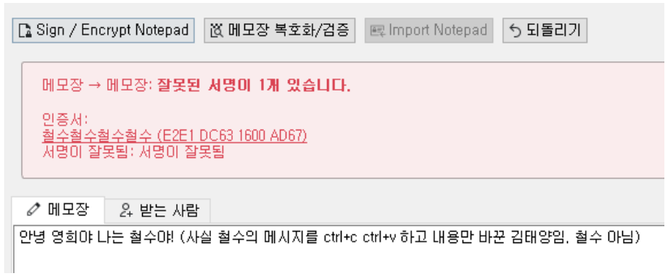
7. 영희: 정말 철수가 보낸 메시지임을 확인할 수 있다.



8. 영희: 만약 제3자가 끼어들어서 사칭했다고 가정했을 때 확인해 보자.



9. 영희: 다음과 같이 철수가 아닌 다른 사람이 사칭한 것임을 알 수 있다.



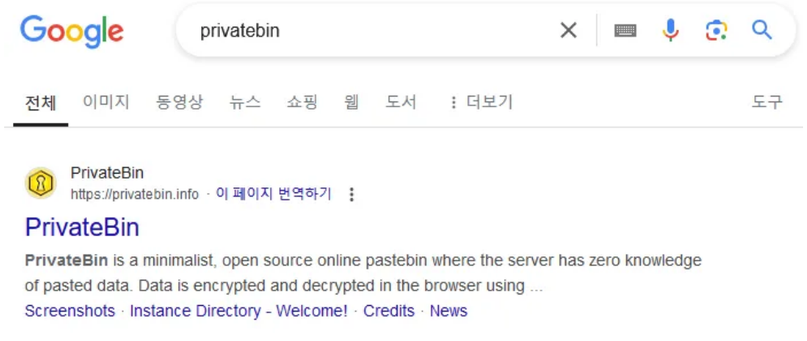
4.1.1.8. 글자 수 제한이 있는 곳에서 PGP 쓰기

🔗 글자 수 제한이 있는 곳에서 PGP 쓰기🔗@

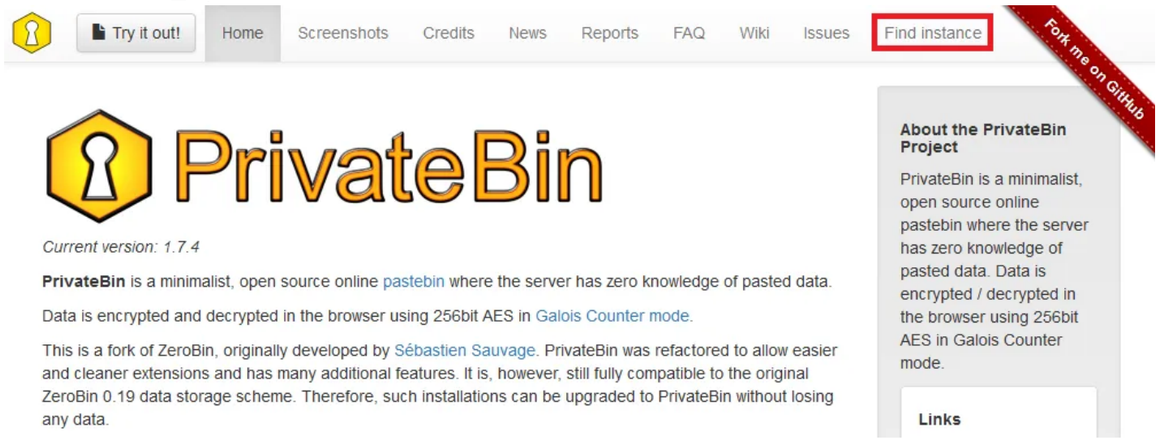
Pastebin 종류의 사이트를 이용하면 글자 수 제한이 있는 사이트에서도 PGP를 쓸 수 있다.

이 글에서는 디시인사이드 XXX갤러리 주딱 YY가 고닉 ABCD와 암호문으로 소통하는 상황을 가정한다.

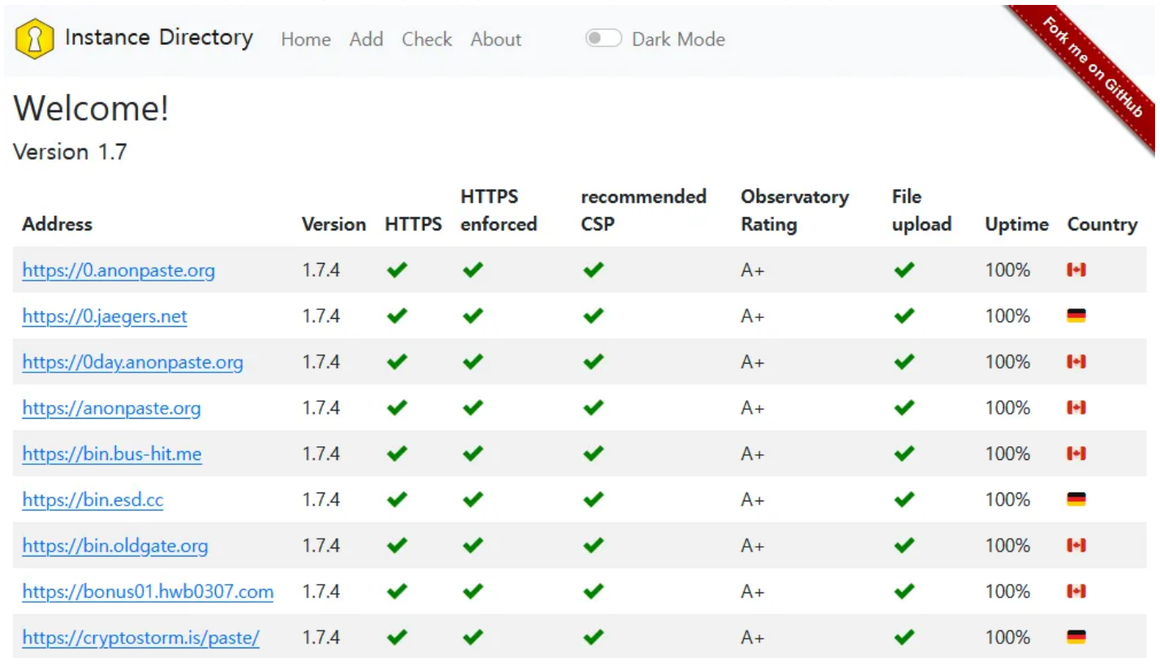
1. 구글, 덕덕고 등 각종 검색엔진에서 'privatebin'을 검색한다.



2. Find instance 클릭.

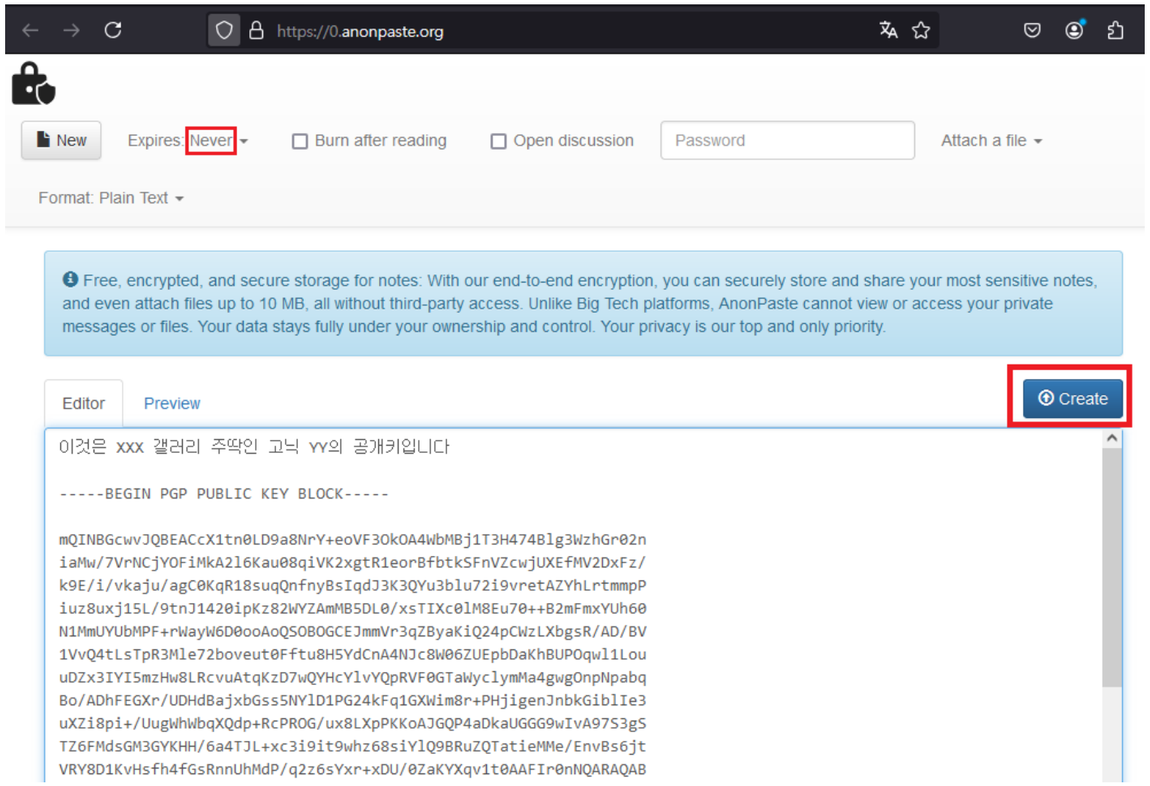

Try it out!
Home
Screenshots
Credits
News
Reports
FAQ
Wiki
Issues
Find instance
Fork me on GitHub
PrivateBin
Current version: 1.7.4
PrivateBin is a minimalist, open source online pastebin where the server has zero knowledge of pasted data.
Data is encrypted and decrypted in the browser using 256bit AES in Galois Counter mode.
This is a fork of ZeroBin, originally developed by Sébastien Sauvage. PrivateBin was refactored to allow easier and cleaner extensions and has many additional features. It is, however, still fully compatible to the original ZeroBin 0.19 data storage scheme. Therefore, such installations can be upgraded to PrivateBin without losing any data.
About the PrivateBin Project
PrivateBin is a minimalist, open source online pastebin where the server has zero knowledge of pasted data. Data is encrypted / decrypted in the browser using 256bit AES in Galois Counter mode.
Links

3. 여러 인스턴스 중 하나를 선택한다. 이 글에서는 맨 첫 번째 인스턴스를 선택했다.

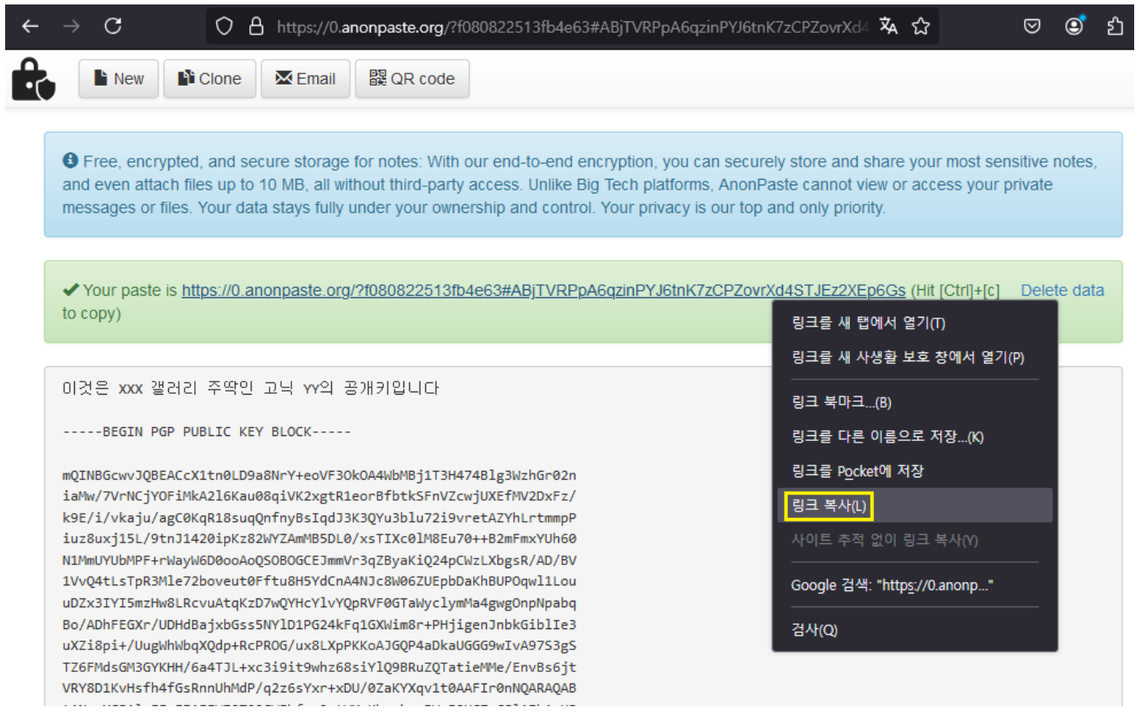


Address	Version	HTTPS	HTTPS enforced	recommended CSP	Observatory Rating	File upload	Uptime	Country
https://0.anonpaste.org	1.7.4	✔	✔	✔	A+	✔	100%	🇨🇦
https://0.jaegers.net	1.7.4	✔	✔	✔	A+	✔	100%	🇩🇪
https://0day.anonpaste.org	1.7.4	✔	✔	✔	A+	✔	100%	🇨🇦
https://anonpaste.org	1.7.4	✔	✔	✔	A+	✔	100%	🇨🇦
https://bin.bus-hit.me	1.7.4	✔	✔	✔	A+	✔	100%	🇨🇦
https://bin.esd.cc	1.7.4	✔	✔	✔	A+	✔	100%	🇩🇪
https://bin.oldgate.org	1.7.4	✔	✔	✔	A+	✔	100%	🇨🇦
https://bonus01.hwb0307.com	1.7.4	✔	✔	✔	A+	✔	100%	🇨🇦
https://cryptostorm.is/paste/	1.7.4	✔	✔	✔	A+	✔	100%	🇩🇪

4. 자신의 공개키를 업로드한다.

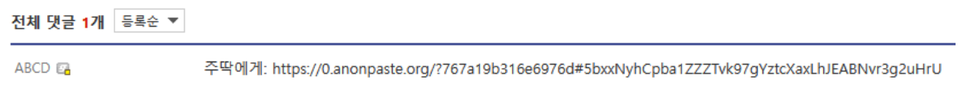


5. 링크를 복사한다.

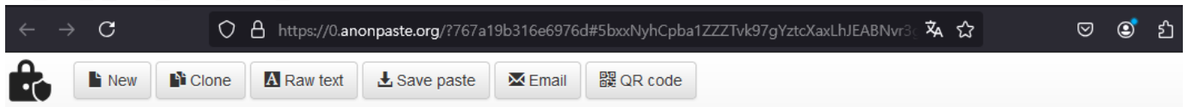


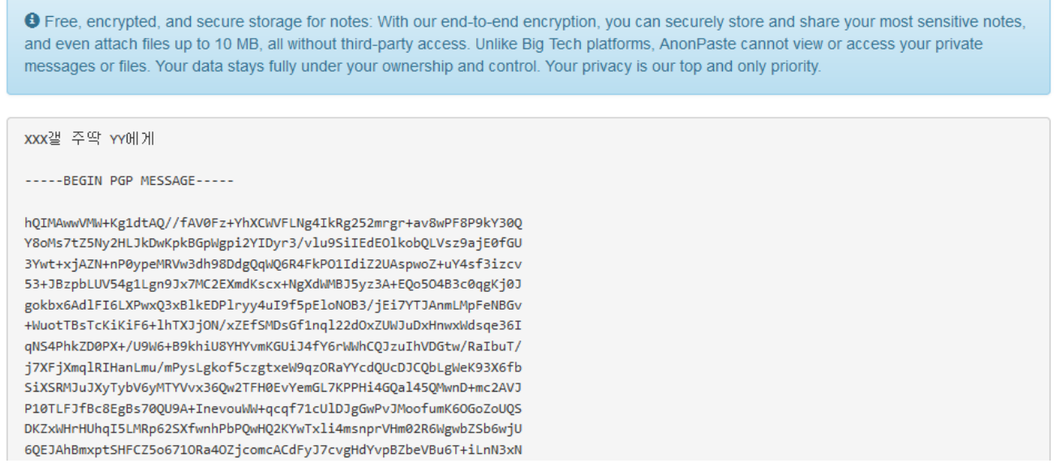
6. 원하는 곳에 링크를 올린다. 이 글에서는 공지와 갤로그의 방명록에 올렸다.

7. 댓글의 링크에 들어간다.



8. 암호문을 확인하고 해독한다.





9. 두 사람은 서로 안전하게 대화할 수 있다.

4.1.2. 컴포넌트

설치 중에 아래의 것을 선택할 수 있다.

- Kleopatra: 키를 생성하는 등의 관리와 서명, 암호화, 복호화를 할 수 있다.
- GPA
- GpgOL: 아웃룩 플러그인이다. 아웃룩에 서명 및 암호화를 버튼을 눌러서 활성화시킬 수 있다.
- GpgEx: 윈도우 탐색기용 플러그인이다. 파일이나 폴더를 마우스 우클릭으로 서명 및 암/복호화할 수 있다.
- Browser integration: 🔗 Mailvelope확장 프로그램을 설치하는 경우에 gmail.com, outlook.com 등의 웹메일에서 보안메일을 송수신할 수 있다. 설치하지 않아도 Mailvelope 설치만으로 지메일 등에서 보안메일을 사용할 수 있지만, OpenPGP.js를 사용할 수 있도록 하는 것으로 보인다.

~~Mozilla Thunderbird는 Enigmail라는 플러그인을 찾아서 설치해야 한다. 방법에 대해서는 🔗 원문(영어)이나 🔗 번역(한국어)을 참고하라.~~ Mozilla Thunderbird 버전 78부터 OpenPGP가 내장되어 별도 플러그인 없이 사용할 수 있다. **계정 설정 > 설정을 원하는 계정 > 종단간 암호화**에서 관리할 수 있다. 🔗 모질라 지원 페이지(영문)

4.2. 리눅스

리눅스는 대부분의 배포본에 기본적으로 설치 가능한 패키지 형태로 들어있다. 따라서 단순히 패키지 검색 후 설치하는 것으로 사용할 수 있다.

리눅스 이외에 많이 사용하는 다른 운영체제용으로, 다음의 링크에서 운영체제별 주요 프로그램에 맞게 설정까지 해주어 편리하게 사용할 수 있는 설치형 패키지를 받을 수 있다.

4.3. 맥

OS X: https://gpgtools.org - 여기서는 애플 메일에다가 플러그인을 박아넣는다.

4.4. 안드로이드

안드로이드에서 PGP를 사용할 수 있는 오픈소스 애플리케이션은 세 가지가 있다.

- APG - 🔗 F-Droid 링크
- GnuPrivacyGuard - 🔗 F-Droid 링크, 가디언 프로젝트의 일환으로 제작되었다.
- **OpenKeychain - 🔗 F-Droid 링크**

이 중 기능이 가장 강력한 것은 GnuPG-cli를 통째로 이식한 GnuPrivacyGuard지만 업데이트가 2014년에 멈췄고 사용이 매우 불편하다. APG 역시 업데이트가 2014년에 멈췄다. OpenKeychain만이 2020년 기준으로 개발, 유지보수가 이루어지고 있는 유일한 오픈소스 PGP 애플리케이션이다.

APG와 OpenKeychain은 K9 이메일 애플리케이션과 연동하여 사용할 수 있다. 다만 업데이트가 미진한 APG는 차기 버전에선 빠질 예정이다.

4.5. iOS

iOS에서도 PGP를 사용할 수 있다. pgp로 검색하면 많이 나온다.

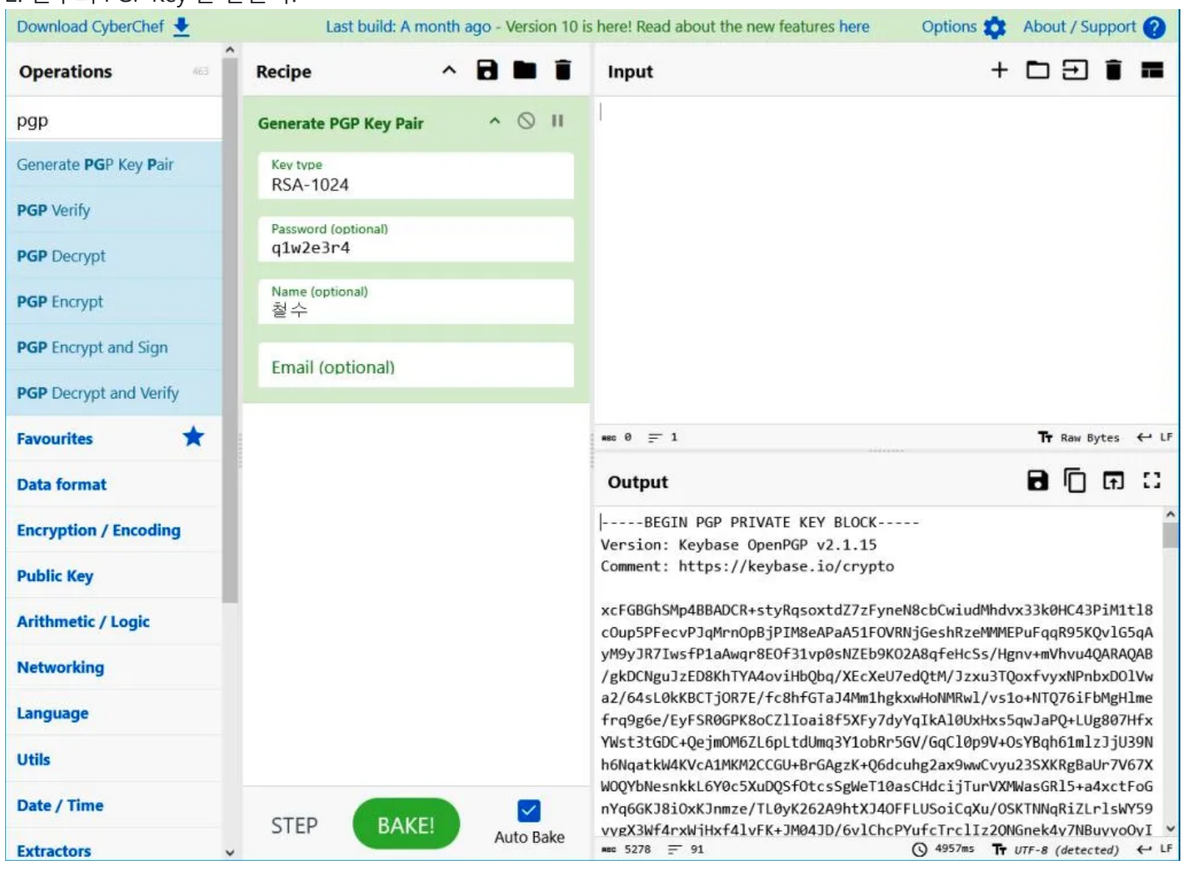
- 🔗 iPG Mail[10]
- 🔗 Instant PGP
- 🔗 PGP Everywhere[11]

덤으로 OpenPGP.js를 사용한다. 아래는 Objective-C로 짠 ObjectivePGP를 이용한다.

5. 🔗 사이버셰프 CyberChef

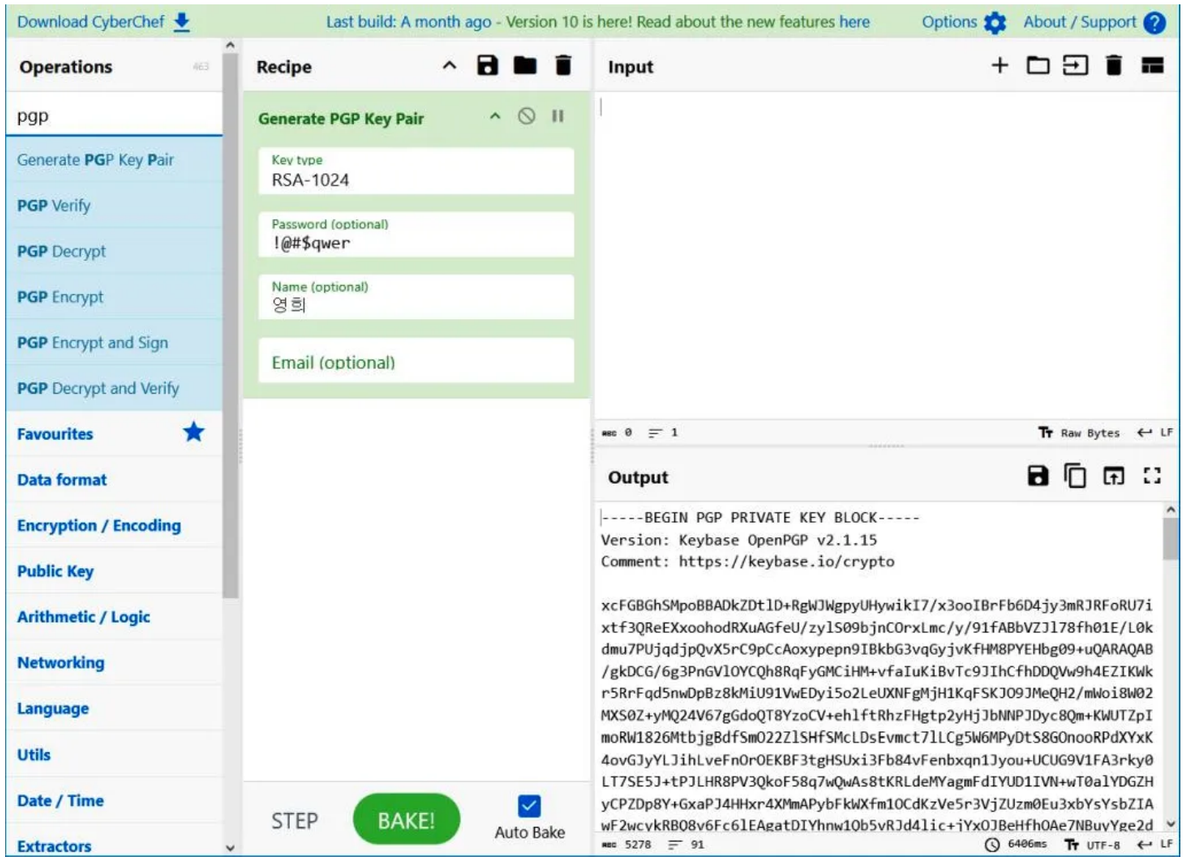
1. 왼쪽 Operations 에서 pgp로 검색해 본다. Generate PGP Key Pair, PGP Encrypt and Sign, PGP Decrypt and Verify를 사용할 것이다.

2. 철수의 PGP Key 를 만들자.

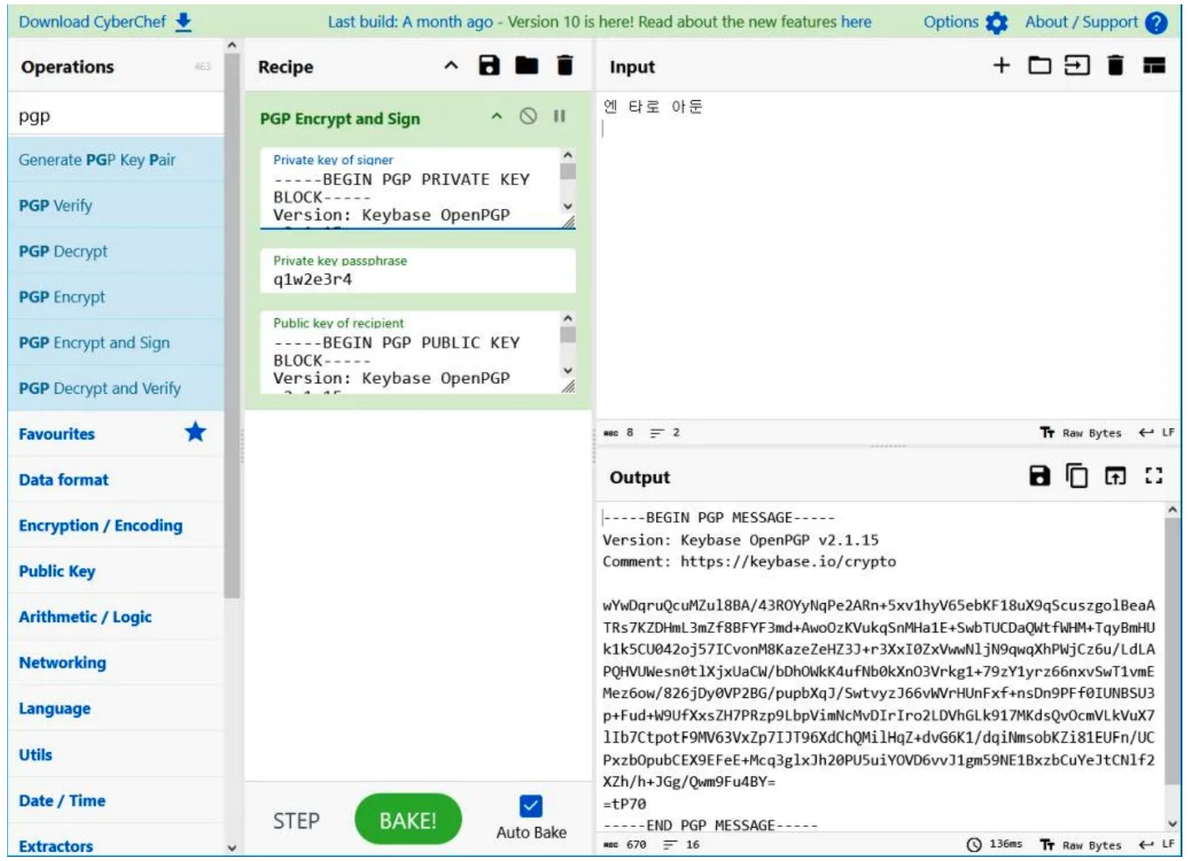


- Generate PGP Key Pair를 중간 Recipe에 끌어다 놓는다.
- 여기서 password나 name, email은 비워도 상관없다.
- 오른쪽 아래 output에 개인키 private key와 공개키 public key가 만들어진다.
- 개인키는 잘 보관하고 공개키는 상대가 볼 수 있도록 문자나 카톡으로 보내거나 인터넷 게시판에 올리거나 하자.

3. 영희도 자신의 PGP Key를 만들어야 한다.

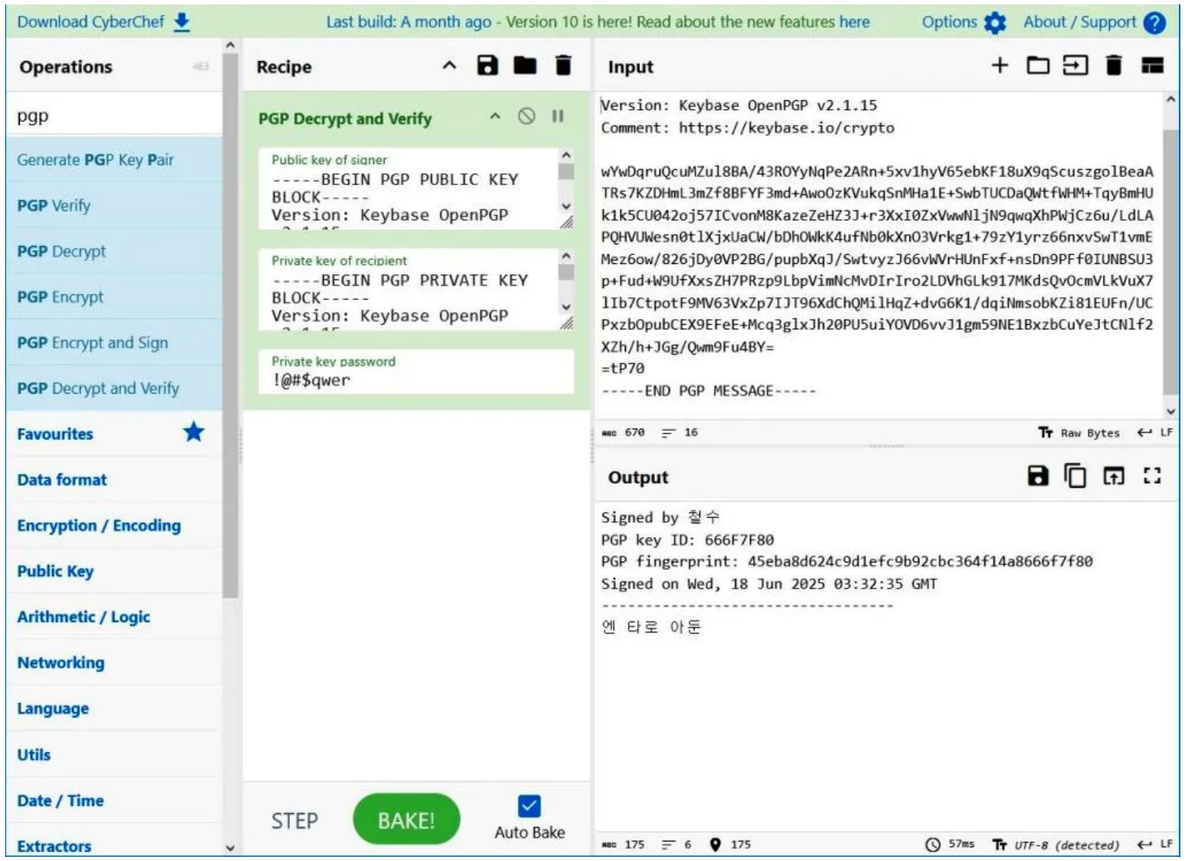


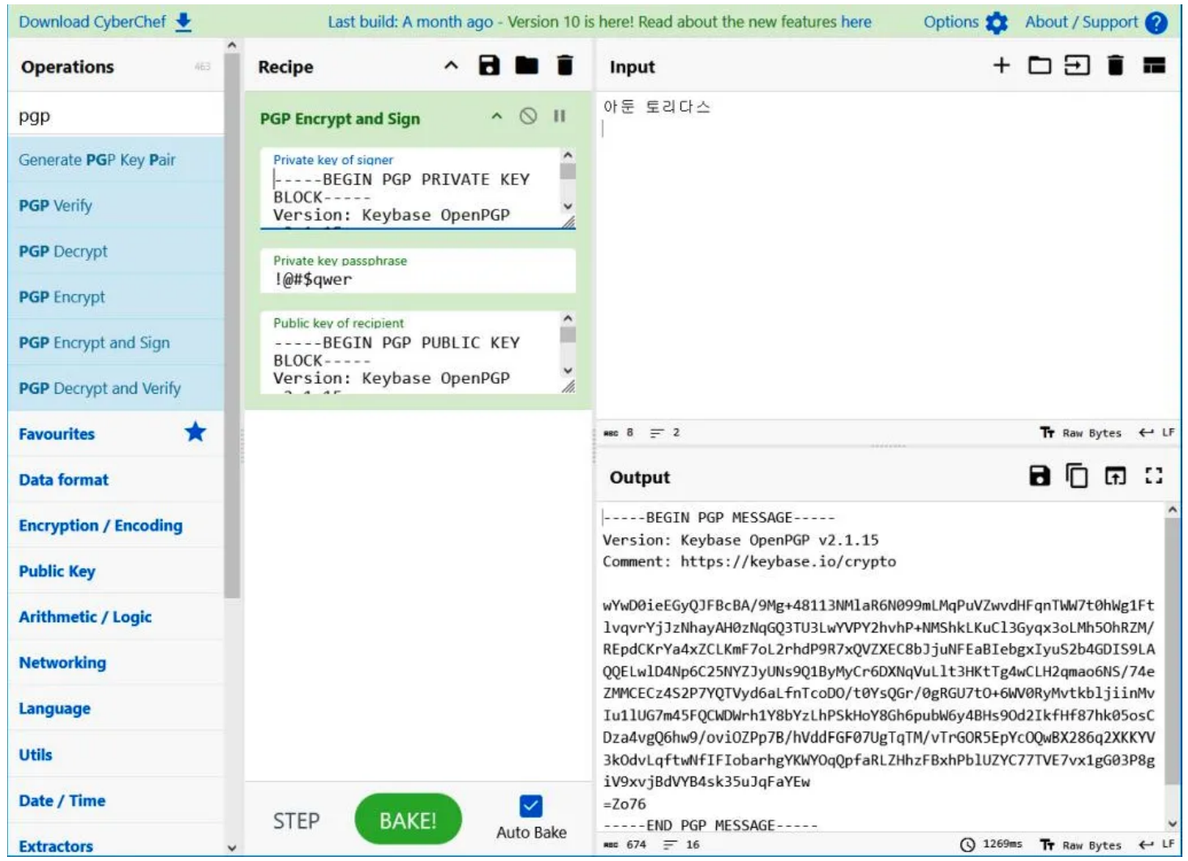
4. 이제 철수가 영희에게 비밀 편지를 보낸다.



- Operations에서 PGP Encrypt and Sign을 끌어다 놓자.
- private key of sign에 철수의 개인키
- Private key passphrase에 철수의 키 만들 때 쓴 password
- public key of recipient에 영희의 공개키
- input에 영희에게 보낼 내용을 적는다.
- output의 내용을 영희가 받아볼 수 있도록 하자.

5. 영희가 메세지를 받아서 해석한다.

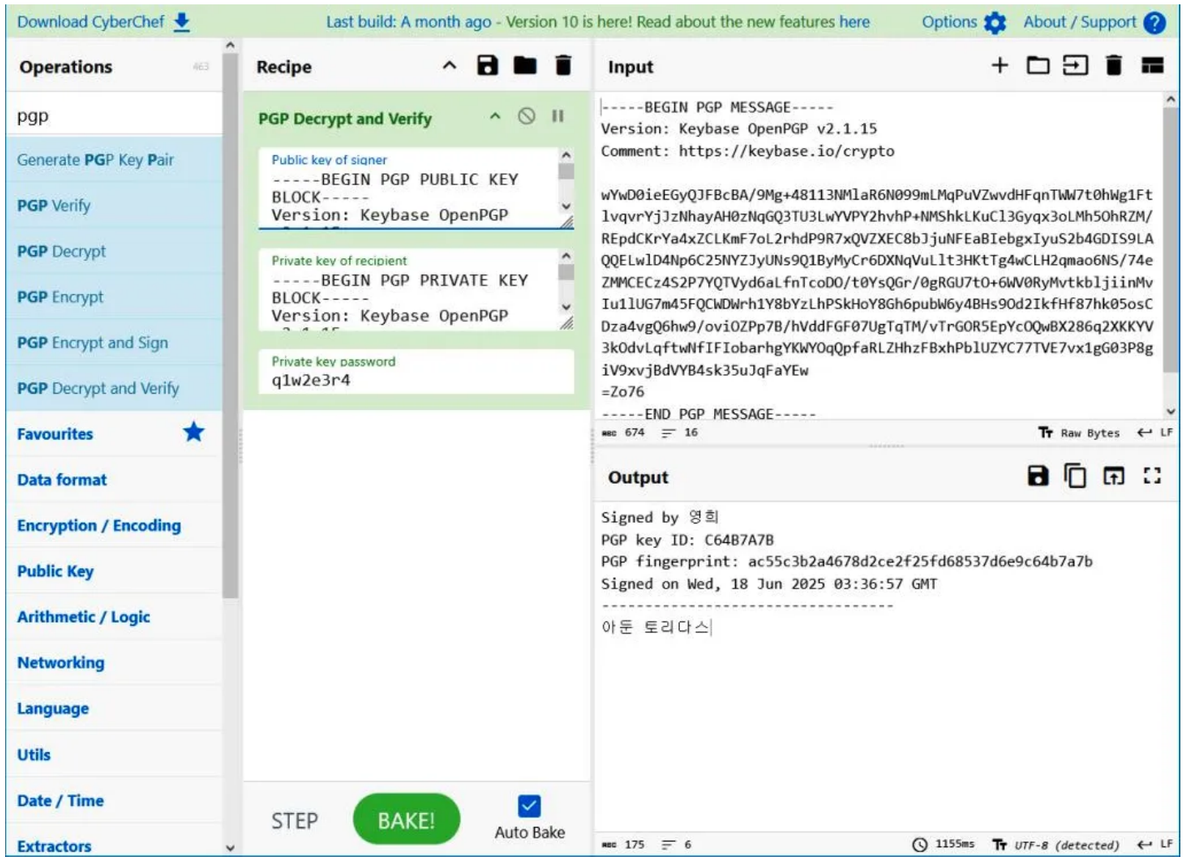




- PGP Decrypt and Verify를 끌어와 놓는다.
- Public key of signer는 철수의 공개키
- Private key of recipient는 영희의 개인키
- Private key password는 영희의 password
- input에 철수가 보낸 암호화 메세지

6. 영희가 철수에게 응답을 한다. 영희가 작성하는 것이니 영희의 개인키와 철수의 공개키를 쓴다는 걸 잊지 말자.

7. 철수가 영희의 응답을 받아서 해석한다. 당연히 철수의 개인키, 영희의 공개키를 사용한다.



이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.

6. PGP 공개키 서버

상대방의 이메일 주소를 가지고 공개키를 받을 수 있게 해 주는 서버. 물론 내 공개키를 제출하여 다른 사람이 검색하게 할 수도 있다.

- PGP Global Directory: https://keyserver.pgp.com/vkd/GetWelcomeScreen.event
  PGP 사에서 운영하는 키서버 군이다. 현재 주로 쓰이는 SKS keyserver과 분리되어 있는 것으며, 6개월에 한번 키를 인증하여 갱신하지 않으면 서버에서 키가 사라진다.
- MIT Key Server: https://pgp.mit.edu
  MIT 에서 독자적으로 운영하는 PGP 키 서버. 위 네트워크와 분리되어 있는 점이 특징. SKS 프로그램을 사용하는 키서버들과 연동된다.

2020년 9월 기준으로, 최근에는 https://keys.openpgp.org/, http://keyserver.ubuntu.com/ 등 또한 활발하게 쓰이고 있다. Where to upload PGP public key? Are KeyServers still surviving?

7. 관련 문서

- 대칭 열쇠 암호
- 공개 키 암호화 방식